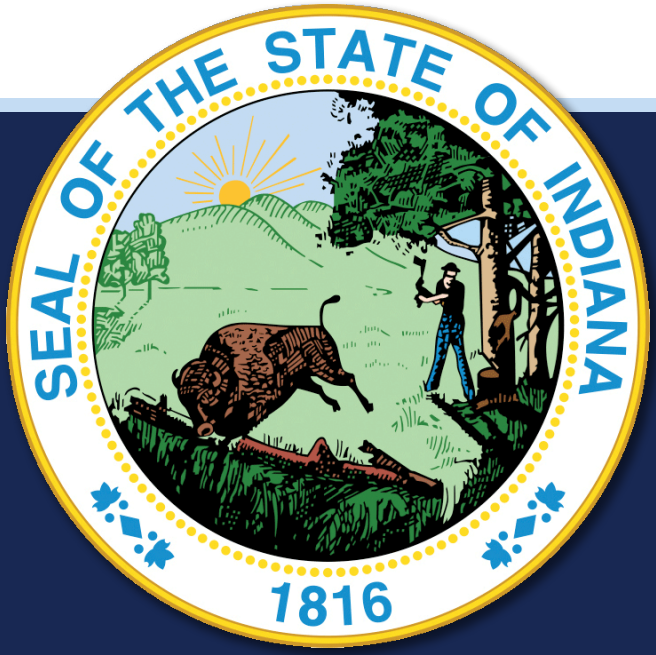
INDIANA CYBERSECURITY STRATEGIC PLAN



September 2018

September 21, 2018

The Honorable Eric J. Holcomb
Governor, State of Indiana
State House, Room 206
Indianapolis, Indiana 46204

Dear Governor Holcomb:

As Indiana's Executive Council on Cybersecurity embarked on taking cybersecurity to the Next Level since your launch in July 2017, it quickly became evident that we had members who not only met the challenge, but exceeded all expectations. It has been an honor to lead such a passionate, expert Council, which has positioned Indiana to have a comprehensive and deep understanding of matters pertaining to cybersecurity.

The efforts of your Council and its first-of-its-kind strategic approach has fostered significant progress in Indiana's cybersecurity planning initiatives. In fact, in the first year the Council already has completed 27.5 percent of its 69 identified deliverables, and 31.6 percent of the stated objectives.

This was not completed by one entity alone. By working collaboratively, Indiana will establish long-term protection strategies that will provide Hoosier residents and businesses with the knowledge and infrastructure needed to be safer from the ever-evolving cyber threats.

As many of the deliverables are being developed and executed by the state and partners, the Council asks for your continued leadership in:

- Supporting of a statewide cybersecurity public relations and awareness campaign;
- Encouraging the highest-level technical and administrative cybersecurity best practices and standards be followed;
- Supporting policy that will boost the cybersecurity posture of Indiana;
- Providing appropriate support to the critical infrastructures as they move forward with their many deliverables;
- Encouraging all of Indiana's workforce ecosystem to follow national standards and develop the cybersecurity pipeline;
- Developing local law enforcement and emergency management in their knowledge to best respond and recover from a cyberattack; and
- Supporting the Council as it moves forward, including ensuring its membership matches the needs of the state.

The following *Indiana Cybersecurity Strategic Plan* encompasses not only the breadth of topics, but also the depth. While the plan in its entirety is large and comprehensive, it is organized so that specific information regarding specific topics can easily be accessed as needed. Each section can stand alone and readers, based on their interests, can select one or a combination of parts of the plan as they aim to learn and further develop solutions addressing cybersecurity in the state.

We appreciate the opportunity to serve Hoosiers and further posture Indiana's cybersecurity strategy, and we look forward to continuing our efforts to supporting the mission of taking cybersecurity to the Next Level.

Sincerely,

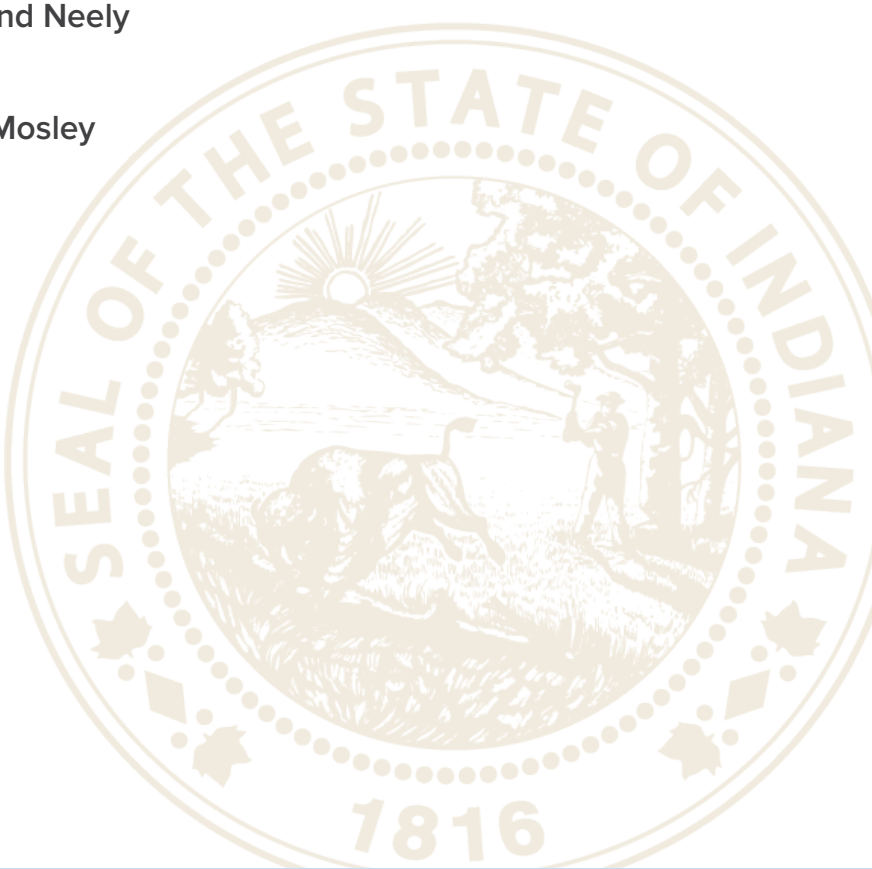
Executive Director Bryan Langley
Indiana Department of Homeland Security

Superintendent Doug Carter
Indiana State Police

Adjutant Major General Courtney Carr
Indiana National Guard

Chief Information Officer and Director Dewand Neely
Indiana Office of Technology

Cybersecurity Program Director Chetrice L. Mosley
State of Indiana



INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

2018 Voting Members

Senior Operations Director Samuel Hyer, Office of Governor Eric J. Holcomb

Chief of Staff Tracy Barnes, Office of Lt. Governor Suzanne Crouch

Executive Director Bryan Langley, Indiana Department of Homeland Security

Chief Information Officer and Director Dewand Neely, Indiana Office of Technology

Superintendent Douglas Carter, Indiana State Police

Adjutant General MG Courtney Carr, Indiana National Guard

Cybersecurity Program Director Chetrice L. Mosley, State of Indiana

Secretary of State Connie Lawson, State of Indiana

Attorney General Curtis Hill, State of Indiana

Chair James Huston, Indiana Utility Regulatory Commission

Commissioner Teresa Lubbers, Indiana Commission for Higher Education

Commissioner Adam Krupp, Indiana Department of Revenue

Secretary of Commerce Jim Schellinger, Indiana Economic Development Corporation

Commissioner Fred Payne, Indiana Department of Workforce Development

Director Danielle Chrysler, Indiana Office of Defense Development

Information Security Officer Owen LaChat, MutualBank

Executive Director Stephen A. Key, Hoosier State Press Association

Partner Ronald W. Pelletier, Pondurance

Information Technology Vice President John Lucas, Citizens Energy Group

President Mark T. Maassel, Indiana Energy Association

Executive Director Rhonda Cook, Accelerate Indiana Municipalities (AIM)

Executive Director Stephanie Yager, Indiana Association of County Commissioners

Chief Information Officer Mark A. Lantzy, Indiana University Health

Executive Director Joni K. Hart, Indiana Cable Telecommunications Association

Business Manager for IT Security David Ehinger, Rolls Royce

Chief Information Officer Brad Wheeler, Indiana University

Chief Information Officer Gerry McCartney, Purdue University

Table of Contents

ABOUT THIS PLAN 7

PART 1 - STRATEGIC FRAMEWORK OF IECC 9
- Today's Cyber Threat 10
- The Solution: Indiana's Commitment to Cybersecurity 10
- Developing the Council and the Strategy 12
- Executive Order Completion 14

PART 2 - IMPLEMENTATION PLAN 16
- Executive Summary of Plans 17
- Observations and Considerations of IECC 26
- 2018 Recommendations 27

PART 3 - YEAR IN REVIEW 28
- 2018 Membership and Leadership 29
- Best Practices of IECC 29
- Deliverables Completed 29
- Additional Accomplishments in Indiana 30
- IECC Moving Forward 32

APPENDICES 33
- Appendix A Indiana Executive Council on Cybersecurity – Executive Order 34
- Appendix B Indiana Executive Council on Cybersecurity – Charter 38
- Appendix C Indiana Executive Council on Cybersecurity – Phase Forms 53

...continued on next page

Table of Contents (continued)

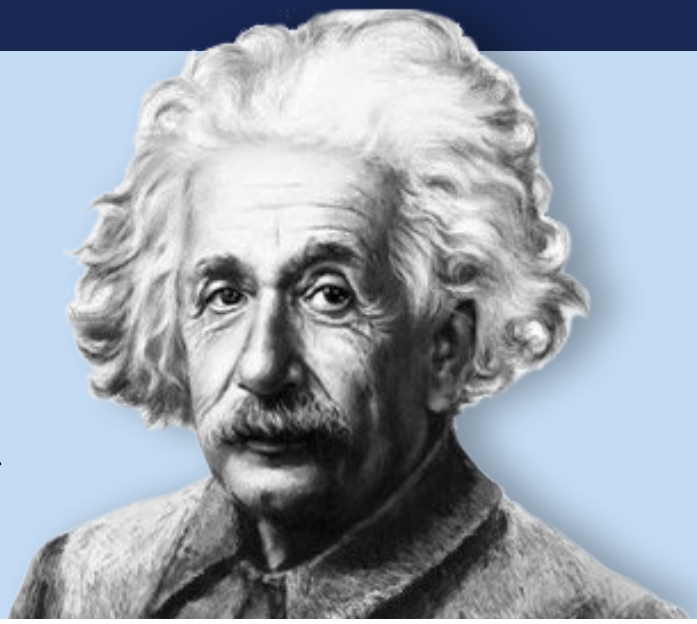
APPENDICES (continued)

Appendix D Indiana Executive Council on Cybersecurity – Committee and Working Group Implementation Plans 86
Appendix D.1 Communications Committee 87
Appendix D.2 Defense Industry Committee 148
Appendix D.3 Economic Development Committee 191
Appendix D.4 Elections Committee 256
Appendix D.5 Energy Committee 689
Appendix D.6 Finance Committee 770
Appendix D.7 Government Services Committee 801
Appendix D.8 Healthcare Committee 838
Appendix D.9 Water & Wastewater Committee 1018
Appendix D.10 Workforce Development Committee 1098
Appendix D.11 Cyber Pre- & Post- Incident Working Group 1174
Appendix D.12 Cyber Sharing Working Group 1303
Appendix D.13 Cyber Summit Working Group 1355
Appendix D.14 Emergency Services & Exercise Working Group 1386
Appendix D.15 Legal & Insurance Working Group 1525
Appendix D.16 Local Government Working Group 1610
Appendix D.17 Personally Identifiable Information Working Group 1633
Appendix D.18 Policy Working Group 1685
Appendix D.19 Public Awareness & Training Working Group 1722
Appendix D.20 Strategic Resource Working Group 2026
Appendix E Indiana Executive Council on Cybersecurity – Membership & Leadership List 2076
Appendix F Indiana Executive Council on Cybersecurity – Executive Order Goals & Deliverables 2085

ABOUT THIS PLAN

"Out of clutter, find simplicity."

-Albert Einstein



The world of cybersecurity is highly complex and cluttered with information, misinformation, and disinformation. As a consequence, it is important to approach it strategically and create simplicity. This has been a key element in determining not only where Indiana's past and current cybersecurity efforts are, but also where the state will go next.

The *Indiana Cybersecurity Strategic Plan* outlines those directions as simply and as directly as the complexity of the effort allows.

This plan is organized into three sections: the Framework, in which the Indiana Executive Council on Cybersecurity (IECC or Council) was built; the detailed Implementation Plans developed by the members; and a Year in Review.

Part One is the Council's strategic framework. It provides the background of the Council, establishes high-level cybersecurity goals, presents the composition of membership, and addresses how it has met the objectives of Indiana Governor Eric J. Holcomb's Executive Order.

Part Two is an executive summary of the implementation plans created by 20 separate committees and working groups, each developed with objectives that are specific, measurable, achievable, and relevant to the overall strategic vision. Additionally, this section contains observations, considerations, and recommendations. Note that each plan is provided in its entirety in the Appendices of this strategic plan.

Part Three presents the 2017-2018 year in review. This section identifies the dedicated members and leaders of the Council who developed these plans, completed deliverables of the first-year plans, contributed to additional accomplishments in Indiana, and advised the Council on how to move forward.

In addition to the aforementioned parts of this plan, the heart of the Indiana Cybersecurity Strategic Plan is Appendix D. These are the 20 detailed implementation plans developed for the respective sectors and areas by the more than 200 members of the Council.

This plan and all the appendices also can be found on www.in.gov/cybersecurity/3842.htm.

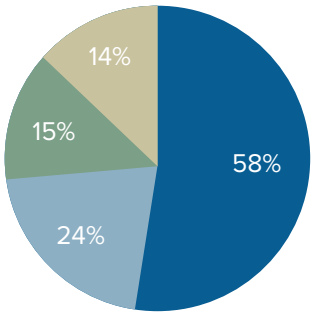
PART 1
STRATEGIC FRAMEWORK OF IECC

TODAY'S CYBER THREAT

Critical infrastructure and key resource sectors rely heavily on information technology to manage complex systems; including public utilities, healthcare, telecommunications, transportation, financial services, manufacturing, education, research, and public safety. The reality of this interconnectivity is that cyber risks grow at an exponential rate and pose a profound risk to citizens, organizations, and industries, as well as threaten the security and economy of Indiana. This is all the more relevant considering the most recent worldwide cyberattacks along with those that have occurred right here in Indiana.

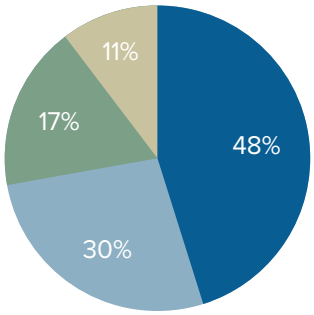
In fact, the 2018 Verizon Data Breach Investigations Report found the victims of breaches to be 58 percent small businesses, 24 percent healthcare organizations, 15 percent accommodation and food services, and 14 percent public sector entities. Of those breaches, 48 percent occurred from hacking, 30 percent included malware, 17 percent were social attacks (such as phishing), and 11 percent involved physical security. Email continues to be the most common method of delivery, accounting for 96 percent of breaches.

2018 BREACH VICTIMS



small businesses
healthcare organizations
accommodation and food services
public sector

2018 BREACH SOURCES



hacking
malware
social attacks (phishing)
physical security

THE SOLUTION

INDIANA'S COMMITMENT TO CYBERSECURITY

As the State of Indiana became more centralized in its information technology, the Indiana Office of Technology began developing its state cyber strategy in two documents: The Cyber Security Framework Strategy (2009) and the Information Security Framework (2013). These documents describe the organization, governance, practices, and policies to be implemented in order to achieve an effective security approach for the state.

Inward focus and inter-agency coordination were intended to protect the state, but more needed to be done to protect the citizens and businesses of Indiana. In August 2015, the Indiana Department of Homeland Security (IDHS) was tasked to conduct additional research and develop a roadmap of how to most effectively collaborate and engage with public and private partners in developing a long-term cyber strategy. This included IDHS leading a first-of-its-kind critical infrastructure tabletop and operational exercise series called Crit-Ex in 2016. This exercise was the first of these cross-sector initiatives (public and private) designed to improve the understanding of Indiana's cyber ecosystem and identify capability gaps. Crit-Ex was planned as a series of exercises that explored the intersection of cybersecurity and critical infrastructure, using scenarios in which a cyberattack on a critical asset leads to physical-world consequences.

The initial phase of Crit-Ex was a six-hour tabletop exercise. The exercise facilitated discussion surrounding the response to a cyberattack resulting in a broad energy disruption, and a myriad of other issues related to the mitigation of such a wide-scale power outage. The tabletop session emphasized the role of local, state, and federal agencies, water/wastewater utilities, and power utilities in response to a coordinated cyber incident that affected the entire State of Indiana.

The second event of the Crit-Ex series was an operational exercise at Indiana National Guard's Muscatatuck Urban Training Center, in which simulated cyberattacks disrupted real-world operational supervisory control and data acquisition (SCADA) systems at a water utility, allowing participants to exercise their cybersecurity response processes. As such, Crit-Ex 2016 was the first-of-its-kind exercise that catalyzed information sharing, training opportunities, partnerships, and response planning across the state.

After this inaugural cyber exercise, it became more evident that securing Indiana's information technology infrastructure and industrial control systems is beyond the reach of any single entity, especially as the nature of the cyber threat came into focus. That is why in March 2016 former-Governor Mike Pence signed an Executive Order establishing the Indiana Executive Council on Cybersecurity (IECC or Council).

The Council was continued on January 9, 2017, through Executive Order 17-11 (See Appendix A), when Governor Eric J. Holcomb took office, with renewed focus on how to build and best utilize the cross-sector body of subject-matter experts to effectively understand Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the convened talent from all sectors to stay on the forefront of the cyber risk environment.

Per Executive Order 17-11, the Council will:

- Develop, maintain, and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe.
- Establish and maintain a strategic framework document that defines high-level cybersecurity goals for the State of Indiana. This framework document shall establish a strategic vision for Indiana's cybersecurity initiatives and detail how the state will:
    - Establish an effective governing structure and strategic direction;
    - Formalize strategic cybersecurity partnerships across the public and private sectors.
    - Strengthen best practices to protect information technology infrastructure;
    - Build and maintain robust statewide cyber incident response capabilities;
    - Establish processes, technology, and facilities to improve cybersecurity statewide;
    - Leverage business and economic opportunities related to information, critical infrastructure, and network security; and
    - Ensure a robust workforce and talent pipeline in fields involving cybersecurity.
- Receive guidance from the Counter-Terrorism and Security Council, which is led by Indiana's Lt. Governor Suzanne Crouch, and report to the Homeland Security Advisor within the Office of the Governor.

Given the challenges and complexities surrounding the directives of the Executive Order, it became imperative to create a strategic framework that would address both statewide and sector-specific topics within the cybersecurity ecosystem. As a result, the State of Indiana hired its first fully dedicated cybersecurity program director in March 2017 to facilitate the Council in fulfilling its purpose. That purpose is to (1) produce an informed overview of Indiana's cyber risks and opportunities; (2) prioritize those items by criticality; and (3) suggest and/or facilitate the implementation of programs/projects designed to achieve associated objectives.

In July 2017, Governor Holcomb launched Version 2.0 of the Council with a new direction in taking cybersecurity to the Next Level in Indiana.

The Council also provides consultative direction on projects, initiatives, and programs, ensuring whole-of-state needs are met and assets are best leveraged. It confirms that these programs align with the unique needs and risk profiles of critical sectors throughout the state and accelerates cyber initiatives and ensure Indiana's cyber stakeholders have the resources and support they need to reach the objectives in cybersecurity.

COUNCIL STATS

YEAR 1

200+ MEMBERS

19 OF 69 DELIVERABLES COMPLETED

38 OF 120 OBJECTIVES COMPLETED

DEVELOPING THE COUNCIL AND THE STRATEGY

COMPOSITION OF THE COUNCIL

To move forward effectively and efficiently, especially given the broad areas and in-depth expertise on the Council, the members were provided with as much information as possible regarding the expectations, processes, roles, and responsibilities of being selected to be a member of the Council. In September 2017, the Voting Members of the Council passed the official Indiana Executive Council on Cybersecurity Charter. This Charter, found in Appendix B, includes the purpose, roles of members and expectations, appointment terms, membership requirements, meeting guidelines, council duties, the strategic breakout of the IECC, and additional provisions.

DEVELOPMENT OF COMMITTEES

The Council was organized into 20 committees and working groups composed of the more than 200 respective members who are experts in their relative fields (See Figure 1). Developing this cybersecurity ecosystem was the only way to achieve maximum results in a relatively short amount of time, but with the depth of knowledge needed to make informed operational decisions.

The IECC Charter was then used to guide the creation of individual committee and working group charters. Each charter clearly defined its goals, members (full time and as needed), and expectations. Moreover, each committee and working group was comprised of members who represented north, central, and southern Indiana as well as small, medium, and large entities, to ensure that diverse input was provided in developing strategic plans. Every committee and working group was chaired by a Voting Member of the Council to ensure that all plans were aligned with the goals of the entire Council.

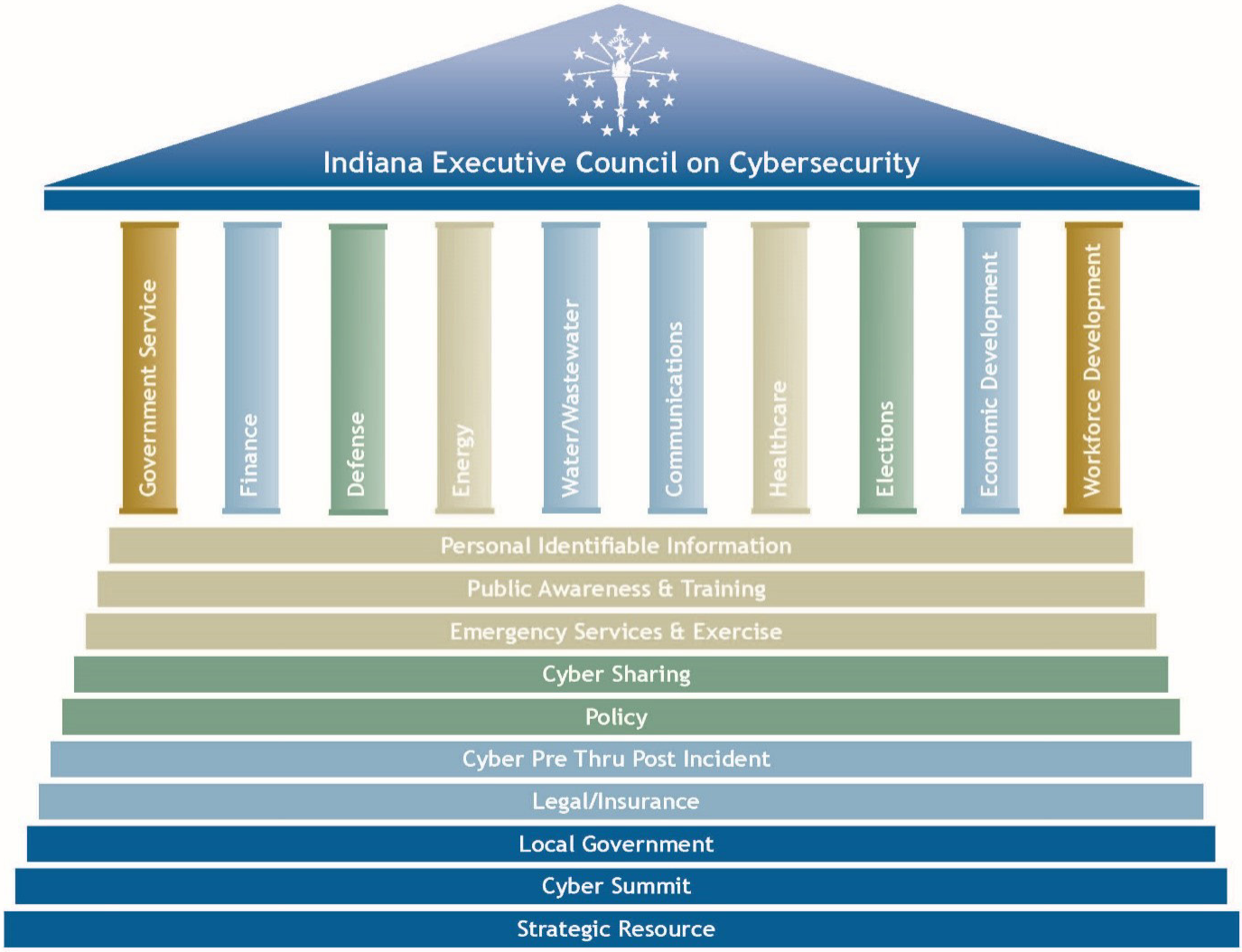


Figure 1 : IECC Strategic Breakdown

THE COUNCIL STRATEGIC PHASES

To guide the work of the 20 committees and working groups in developing a strategic plan, phases were established for each group to follow and complete concurrently. The four key phases were:

Phase 1	Research
Phase 2	Planning
Phase 3	Implementation
Phase 4	Evaluation

PHASE 1 - RESEARCH

Complete questionnaire, primary and/or secondary research

Develop preliminary deliverables and research findings

PHASE 2 - PLANNING

Select and finalize deliverables

Ensure all deliverables tied back to a specific goal of the Executive Order

Develop objectives to drive metrics

PHASE 3 - IMPLEMENTATION

Indicate further details of each deliverable including budget, tactics, resources, timeline, pilot/example products, etc.

PHASE 4 - EVALUATION

Determine the objectives of each deliverable, and methods of evaluating

In addition, meetings, facilitated discussions, director oversight, shared online platforms, and tools, were implemented to avoid duplication of developments and deliverables, and to allow for a fully transparent process. This included a consolidated Q&A forum document that was used within and across the 20 committees and working groups to best and most effectively facilitate communications. For the templates used to assist with each Phase of the committees and working groups, see Appendix C.

EXECUTIVE ORDER COMPLETION

Executive Order (EO) 17-11 provided clear direction for the Council's focus in the coming years. Table 1 (following page) indicates the specific deliverables established within the Governor's Executive Order, the primary owners responsible for completing the requirements, as well as the month in which the performance measure was satisfied.

Table 1 : Governor's Executive Order Deliverables

EXECUTIVE ORDER REQUIREMENT	PRIMARY OWNER(S)	PERFORMANCE MEASURE
Continuance of Council and membership composition met. (EO Sections 1-5)	Indiana Department of Homeland Security, Indiana State Police, Indiana Office of Technology, Indiana National Guard, and Indiana Cybersecurity Program Director	July 2017 – Governor Holcomb and leadership launch Version 2.0 of Council with required membership.
Establish and maintain a strategic framework document that defines high-level cybersecurity goals for the state. This framework document shall establish a strategic vision for state cybersecurity initiatives and detail how the state will meet seven specific goals. (Section 6)	Indiana Cybersecurity Program Director and Voting Members of Council	September 2017 – Passed IECC Charter September 2018 – Submitted final strategic plan that addresses how each deliverable meets at least one of the specific goals in the Executive Order.
Deliver, maintain, and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe. (Section 7)	Council committees and working groups	September 2018 – Committees and working groups each submitted strategic plans that provide objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe.
Receive Guidance from the Counter-Terrorism and Security Council (CTASC) and report to the Homeland Security Advisory with the Office of the Governor. (Section 8)	Indiana Cybersecurity Program Director	July 2017 thru September 2018 – Provided updates to CTASC members, Lt. Governor's Office, and the Homeland Security Advisor.
All state agencies, departments, commissions, bureaus, institutions, and entities shall cooperate to the fullest extent possible with the Executive Order. (Section 8)	Council Members	July 2017 thru September 2018 – All members in good standing have participated to the fullest extent possible per the Executive Order.
Council shall be staffed by the Indiana Department of Homeland Security and subject to the requirements as well as the security and confidentiality expectations under Open Door Law and the Access of Public Records Act. (Section 9 and 10)	Indiana Department of Homeland Security and Indiana Office of Technology	January 2017 thru September 2018 - Indiana Department of Homeland Security has partnered with the Indiana Office of Technology to ensure the Council is staffed, provides the necessary resources, and meets the objectives. Furthermore, the Council including all committees and working groups complied with the Open Door Law and the Access of Public Records Act.

PART 2
IMPLEMENTATION PLANS

EXECUTIVE SUMMARY OF PLANS

Using the strategic framework, and operating within the four phases (research, planning, implementation, and evaluation), the 20 committees and working groups each developed a comprehensive strategic implementation plan that collectively resulted in 69 detailed deliverables and 120 objectives. The majority of the deliverables are being completed by the Council members, whose accomplishments were the result of dedicated state resources assisted by federal and military subject matter experts. Local government entities, academia, and private sector organizations also contributed a considerable amount of donated services, time, and resources.

COUNCIL STATS

- YEAR 1
- 200+ MEMBERS
- 19 OF 69 DELIVERABLES COMPLETED
- 38 OF 120 OBJECTIVES COMPLETED

The following is a list of each committee and working group with their respective deliverables and objectives. Note all deliverables that require additional resources or funding are further detailed in the respective committee or working group plan (see Appendix D). It is also important to note that funding discussed may come from a variety of sources including but not limited to grants, federal, private, public, and academic monies. Moreover, the availability of funding and resources may change as this plan is updated and implemented.

COMMUNICATION COMMITTEE

Deliverable: Establish Voluntary Industry Contact List

- Objective 1: Develop a form and process to collect a central cyber industry contact list by October 2018.
- Objective 2: Seventy percent of all communications providers complete annual cyber contact form by December 2018.

Deliverable: Terminology Glossary

- Objective 1: Complete Communications Sector Terminology Glossary by August 2018. *Completed.*
- Objective 2: Publish Communications Sector Terminology Glossary to IECC website by September 2018. *Completed.*

Deliverable: Cyber Incident Response Engagement Guide

- Objective 1: Develop the Communications Sector Engagement Guidance by October 2018.
- Objective 2: Distribute the Communications Sector Engagement Guidance to 80 percent of identified industry and key stakeholders by November 2018.

Deliverable: Communications Sector White Paper

- Objective 1: Complete the Communications Sector Whitepaper for the industry by October 2018.
- Objective 2: Distribute the Communications Sector Whitepaper to 80 percent of identified industry and key stakeholders by November 2018.

DEFENSE INDUSTRIAL COMMITTEE

Deliverable: Cyber Digital Platform

- Objective 1: Indiana Office of Defense Development and partners will develop a pilot of the Indiana defense cybersecurity market development and capture plan and system (Digital Platform) by August 2018. *Completed.*
- Objective 2: Indiana increases to 2 percent (about $300M) of the Department of Defense (DOD) cybersecurity market share ($15B plus) by FY 2022.

Deliverable: Cyber Market System

- Objective 1: Indiana Office of Defense Development (IODD) and partners will develop and implement a cybersecurity market pursuit plan and system by January 2019.

Deliverable: Cyber Statewide Testbed

- Objective 1: Establish a nationally recognized cybersecurity test bed in Indiana by January 2020.
- Objective 2: Indiana captures 5 percent of international cybersecurity market share of cybersecurity test, training, and demonstration plan and capability by December 2023.

ECONOMIC DEVELOPMENT COMMITTEE

Deliverable: Incentive Program

- Objective 1: IECC Economic Development Committee will propose a list of possible incentive programs to be considered by the State of Indiana by April 2019.
- Objective 2: State of Indiana will establish an incentive program in Indiana by July 2020.

Deliverable: Cybersecurity SIoT Innovation District

- Objective 1: Economic Development Committee will develop business plan recommendations for first cybersecurity/Security in the Internet of Things (SIoT) innovation district by end of August 2019.
- Objective 2: State establishes first cybersecurity/Security in the Internet of Things (SIoT) innovation district, provided appropriate funding source made available, by December 2019.

Deliverable: Implementation Plan for Cybersecurity - Marketing

- Objective 1: Indiana Economic Development Corporation will develop a two-year marketing plan focusing on economic development and Indiana's cybersecurity posture by August 2019.
- Objective 2: Indiana Economic Development Corporation will execute a two-year marketing plan focusing on economic development and Indiana's cybersecurity posture beginning in 2020.

ELECTION COMMITTEE

Deliverable: Statewide Voter Registration System (SVRS) Cybersecurity Enhancements

- Objective 1: Indiana Secretary of State Office will begin utilizing additional security protocols in 2018. *Completed.*

Deliverable: Statewide Voter Registration System (SVRS) user access control enhancement.

- Objective 1: SOS Office and Indiana Election Division will implement the Statewide Voter Registration System (SVRS) user access/authentication upgrades with 100 percent of counties by January 2018. *Completed.*
- Objective 2: SOS Office and Indiana Election Division will launch a Two-Factor Authentication Token Pilot by March 2018. *Completed.*

- Objective 3: SOS Office and Indiana Election Division will provide a report on Two-Factor Authentication Token Pilot by May 2018. *Completed.*

Deliverable: Election System Physical and Logical Security Controls

- Objective 1: Indiana Voting System Technical Oversight Program will develop and distribute the Best Practices for Voting System Logical and Physical Security Manual to all Indiana counties in 2018. *Completed.*

Deliverable: Post-Election Risk Limiting Audit (RLA) Standards and Pilot Program

- Objective 1: Indiana Voting System Technical Oversight Program (VSTOP) will develop and implement an RLA pilot in Marion County by July 2018. *Completed.*
- Objective 2: Indiana Voting System Technical Oversight Program (VSTOP) will provide a report by August 2018 on the July 2018 RLA pilot in Marion County. *Completed.*

Deliverable: Cyber Threat Awareness and Training for County Election Administrators

- Objective 1: Indiana Secretary of State will implement and deliver a multi-year cybersecurity public awareness plan beginning in 2018. *Completed.*
- Objective 2: Eighty percent of Indiana election officials participate in state-offered training by November 2019.
- Objective 3: See a 30-percent decrease in click-through rates of Indiana election officials in State phishing campaign by April 2019.

Deliverable: Election Day Cybersecurity Tabletop Exercises

- Objective 1: Indiana Secretary of State will develop and deliver a training exercise program for election officials and administrators by October 2018.
- Objective 2: Secretary of State will conduct a tabletop election exercise by April 2019.

Deliverable: Indiana Best Practices Manual for the Operation of Election Equipment

- Objective 1: Indiana Voting System Technical Oversight Program (VSTOP) will develop the Indiana Best Practices Manual for the Operation of Election Equipment by July 2018. *Completed.*

Deliverable: Election Day Cybersecurity Emergency Preparedness Plans

- Objective 1: Indiana Secretary of State and Election Division will provide existing Election Day emergency preparedness and response material to include cybersecurity for distribution prior to May 2018. *Completed.*

Deliverable: Election Day Cybersecurity Monitoring and Rapid Response Technical Support

- Objective 1: Secretary of State will develop and implement an Election Day cybersecurity technical support program by April 2018. *Completed.*
- Objective 2: Secretary of State will develop an Election Day cybersecurity technical support program report and after action review with key partners by October 2018.

Deliverable: Election Cybersecurity Public Education and Awareness

- Objective 1: Secretary of State will develop a communications plan specific to election security by April 2018. *Completed.*
- Objective 2: Secretary of State will measure the success of communication plan efforts specific to election security by October 2018.

Deliverable: Election Cybersecurity Incident Response and Communications

- Objective 1: Secretary of State will develop and distribute an Election Day cybersecurity incident communications and response to all Indiana election county officials by October 2018.

Deliverable: Catalog and Summaries of Best Election Cybersecurity Reports and Guides

- Objective 1: Secretary of State will develop an election cybersecurity library by October 2018.

ENERGY COMMITTEE

Deliverable: Critical Infrastructure Information (CII)

- Objective 1: IECC Energy Committee will provide current definitions and review of potential policy changes to protect critical infrastructure information while maintaining public access and freedom of information by July 2018. *Completed.*

Deliverable: Contacts

- Objective 1: More than 85 percent of Indiana electric and natural gas utilities will provide the Indiana Utility Regulatory Commission's Emergency Support Function lead, on behalf of the Indiana Department of Homeland Security, a cybersecurity contact by June 2018. *Completed.*
- Objective 2: The Indiana Utility Regulatory Commission's Emergency Support Function lead will maintain the cyber contact list on behalf of the Indiana Department of Homeland Security Emergency Operations Center annually. *Completed.*

Deliverable: Coordinate with Others

- Objective 1: IECC Energy Committee will coordinate with other committees and working groups as needed to effectively complete the State Cybersecurity Strategic Plan by September 2018. *Completed.*
- Objective 2: IECC Energy Committee will share information with Energy Information Sharing and Analysis Center (ISAC) regarding Indiana's new cyber sharing resources by December 2018.

Deliverable: Metrics

- Objective 1: IECC Energy Committee will provide the utility energy industry an annual survey that will assess cybersecurity planning, preparedness, and recovery posture by June 2018. A summary of the results from all survey responses will be sent to the IECC. *Completed.*
- Objective 2: Eighty percent of all utilities will complete annual survey by July 2018. The actual result was 100 percent participation with all responses received prior to June 2018. *Completed.*

Deliverable: Training

- Objective 1: IECC Energy Committee will provide the IECC Workforce Development Committee the needs of the energy sector, as well as examples to consider, as Indiana cybersecurity training and apprenticeship programs are being developed by July 2018. *Completed.*

FINANCE COMMITTEE

Deliverable: Cyber Training (Ivy Tech)

- Objective 1: Ivy Tech will develop a cybersecurity curriculum for business executives by July 2018. *Completed.*
- Objective 2: IECC Finance Committee and Ivy Tech will launch a pilot program with seven participants by August 2018. *Completed.*

Deliverable: Top Security Tips Material

- Objective 1: IECC Finance Committee will develop the Top Information Security Tips training material for Indiana businesses by December 2018.

GOVERNMENT SERVICE COMMITTEE

Deliverable: Indiana's Cybersecurity Hub Website

- Objective 1: IECC will develop and launch a statewide cyber hub website by September 2018. *Completed.*
- Objective 2: Increase website traffic to www.in.gov/cyber by 200 percent by September 2019.

Deliverable: Indiana Cyber Disruption/Emergency Plan

- Objective 1: IECC Government Services Committee will develop the Indiana Cyber Disruption/ Emergency Plan for the public by May 2019.

HEALTHCARE COMMITTEE

Deliverable: Long-term Education

- Objective 1: IECC Healthcare Committee will create Indiana-focused versions of security education by March 2019.
- Objective 2: Provide Indiana-focused versions of security education to 80 percent of Indiana healthcare providers by May 2019.

Deliverable: Indiana Threat Intelligence Distribution System

- Objective 1: Develop a pilot program with three participants of the Indiana Health Cyber Threat Intel Committee by November 2018.
- Objective 2: Evaluate pilot program and recommend a sustainability framework model for the state of Indiana to maintain by February 2019.

Deliverable: Vendor Management

- Objective 1: Create vendor management resources for healthcare providers by February 2019.
- Objective 2: Distribute vendor management resources to 80 percent of healthcare providers by April 2019.

WATER & WASTEWATER COMMITTEE

Deliverable: Cyber Risk Model (Plan)

- Objective 1: IECC Water and Wastewater Committee and partners develops a Cyber Plan Template for Indiana water/wastewater companies by December 2018.
- Objective 2: IECC Water and Wastewater Committee and partners distributes the Cyber Plan Template to 25 percent of Indiana water/wastewater companies by March 2019.

Deliverable: Cyber Contacts

- Objective 1: Indiana Department of Environmental Management will conduct modifications to the Safe Drinking Water Information System to collect cybersecurity contact information for Indiana water and wastewater organizations by November 2017. *Completed.*
- Objective 2: Indiana Department of Environmental Management will maintain the cybersecurity contact information for 95 percent of Indiana water organizations serving a population greater than 3,301 by December 2019.

Deliverable: Risk Tool

- Objective 1: IECC Water and Wastewater Committee develops the Cyber Assessment Risk Tool within 12 months of securing funding.
- Objective 2: Eighty percent of Indiana water and wastewater companies will have used the Cyber Assessment Risk Tool within 24 months of deployment.

Deliverable: Training Plan

- Objective 1: IECC Water and Wastewater Committee will develop a training plan within three months of securing funding.
- Objective 2: Fifty percent of Indiana water and wastewater companies will incorporate the training plan as a part of their operational resources within 24 months of deployment of the training plan.

Deliverable: Cyber Plan Template

- Objective 1: IECC Water and Wastewater Committee will develop a Cyber Plan Template for Indiana water/wastewater companies by April 2019.
- Objective 2: IECC Water and Wastewater Committee and partners will distribute the Cyber Plan Template to 50 percent of Indiana water/wastewater companies by October 2019.

WORKFORCE DEVELOPMENT COMMITTEE

Deliverable: Generate Interest Plan

- Objective 1: Establish and fund a statewide cybersecurity program for K-12 stakeholders by July 2019.
- Objective 2: Launch a statewide cybersecurity program for K-12 stakeholders by August 2019.

Deliverable: Job Demand Tool

- Objective 1: State of Indiana adopts Cyberseek as the source for cybersecurity-related job demand and career pathways for the state by August 2019.
- Objective 2: State of Indiana will develop integration plans for consumption of the Cyberseek.org data across various job seeker, employer, and education platforms by December 2019.

Deliverable: K-12 Offering Cybersecurity Content

- Objective 1: Indiana Department of Education will develop a menu of cybersecurity content and initiatives that includes K-12 computer science offerings by September 2019.
- Objective 2: Eighty percent of Indiana Schools adopt one or more cyber initiatives by August 2020.

Deliverable: Best Practices and NICE Framework Standard

- Objective 1: Indiana formally establishes NICE Framework as the cybersecurity standard for the state by October 2019.
- Objective 2: Working with the National Governors Association, the IECC Workforce Development Committee will create and implement statewide program that will provide educators and businesses resources for meeting best practices and standards, such as the NICE Framework, by December 2019.
- Objective 3: Working with the National Governors Association, the IECC Workforce Development Committee will create and implement statewide outreach program for cybersecurity training that follows best practices and standards, such as the NICE Framework, to underserved communities, minorities, women, veterans, disables, and minor offenders by December 2019.

Deliverable: Incentivized Cybersecurity Certifications

- Objective 1: Indiana Department of Workforce Development and partners will create and launch a statewide cybersecurity certification training program that meets NICE standards by December 2019.

Deliverable: Program Data Tool

- Objective 1: Indiana Commission for Higher Education will develop and launch a survey for post-secondary to report on cybersecurity-related programs by March 2019.
- Objective 2: Indiana Commission for Higher Education will develop and deliver a final report to the IECC on findings of post-secondary survey by December 2019.

CYBER PRE- & POST- INCIDENT WORKING GROUP

Deliverable: Exercise

- Objective 1: State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Exercise by December 2020.

Deliverable: Gap Analysis

- Objective 1: IECC Cyber Pre- thru Post-Incident Working Group will complete a comprehensive gap analysis of identified high-risk critical infrastructure sectors by August 2018. *Completed.*
- Objective 2: IECC Cyber Pre- thru Post-Incident Working Group will provide recommendations based on a comprehensive gap analysis of identified high-risk critical infrastructure sectors by December 2018.

Deliverable: Cyber Emergency Response Team (IN-CERT)

- Indiana State Police will develop and launch Indiana Cyber Emergency Response Team training program within 12 months of the Council partners securing an encumbered source of funding.

Deliverable: Cyber Assessments

- Objective 1: Indiana National Guard will develop a Local/State Government Cyber Assessment Program by December 2018.
- Objective 2: Indiana National Guard will conduct Cyber Assessment for State critical infrastructure entities by December 2019.

CYBER SHARING WORKING GROUP

Deliverable: Best Practices

- Objective 1: IECC Cyber Sharing Working Group will create a list of best practices by January 2019.

Deliverable: Cyber Sharing Maturity Model

- Objective 1: IECC will develop Indiana's first cyber sharing maturity model by February 2019.
- Objective 2: IECC will distribute Indiana's first cyber sharing maturity model to critical infrastructures through 90 percent of Indiana associations by June 2019.

Deliverable: Inventory of Cyber Sharing Resources

- Objective 1: IECC Cyber Sharing Working Group will complete an inventory of cyber sharing resources by July 2018. *Completed.*

Deliverable: MS-ISAC Member Recruitment

- Objective 1: Increase Indiana MS-ISAC membership by 25 percent by June 2019.

Deliverable: Secured Information Sharing Program

- Objective 1: IECC Cyber Sharing Working Group will develop a Secured Information Sharing Program by July 2019.
- Objective 2: IECC Cyber Sharing Working Group will launch a Security Information Sharing Program by August 2019.

CYBER SUMMIT WORKING GROUP

Deliverable: Cybertech Midwest

- Objective 1: IECC will secure a cybersecurity conference partner for three years by May 2018. *Completed.*
- Objective 2: State of Indiana will hold its first statewide cybersecurity conference by October 2018.

EMERGENCY SERVICES & EXERCISE WORKING GROUP

Deliverable: Annex

- Objective 1: Indiana Department of Homeland Security (IDHS) will develop and distribute the state's Comprehensive Emergency Management Plan (CEMP) Cyber Annex to appropriate parties by December 2018.
- Objective 2: IDHS will exercise the CEMP Cyber Annex by December 2019.

Deliverable: IDHS Cyber Exercise Engagement

- Objective 1: IDHS will develop and launch Cyber Exercise Engagement Program by July 2019.

Deliverable: Toolkit

- Objective 1: IECC Emergency Services and Exercise Working Group will develop a Cyber Response Toolkit Version 1.0 by October 2018.
- Objective 2: IDHS will launch four workshops throughout Indiana using the Cyber Response Toolkit by October 2019.
- Objective 3: Partnering with the National Governors Association, the IECC Emergency Services and Exercise Working Group will develop a Cyber Response Toolkit 2.0 with a cyber risk tool for emergency personnel by August 2019.
- Objective 4: IDHS will develop and launch four workshops throughout Indiana using the Cyber Response Toolkit 2.0 by March 2020.

Deliverable: EOC

- Objective 1: IDHS will develop a Cyber Liaison position within its Emergency Operations Center by May 2019.
- Objective 2: IDHS will complete training and exercise the Cyber Liaison position within the EOC by December 2019.

LEGAL & INSURANCE WORKING GROUP

Deliverable: Insurance Guide

- Objective 1: IECC Legal and Insurance Working Group will develop a Cyber Insurance Guide to be provided to government and businesses by September 2018. *Completed.*

Deliverable: Policy Review

- Objective 1: Legal and Insurance Working Group will develop a list of cyber laws applicable to Indiana businesses and residents under the current landscape by August 2018. *Completed.*

Deliverable: Cyber Insurance Survey

- Objective 1: Legal and Insurance Working Group will conduct a survey of businesses for insurance coverage and cybersecurity insurance coverage by August 2019.
- Objective 2: Legal and Insurance Working Group will provide a report of the findings of the cyber insurance survey to the IECC by December 2019.

LOCAL GOVERNMENT WORKING GROUP

Deliverable: Local Officials Cybersecurity Guidebook

- Objective 1: Develop a guidebook for local government officials to assist them with cybersecurity planning and education expected by fall of 2018.
- Objective 2: Promote guidebook on cybersecurity planning and education to local government officials throughout 2019.

PERSONAL IDENTIFIABLE INFORMATION WORKING GROUP

Deliverable: Indiana PII Guidebook

- Objective 1: IECC PII Working Group will develop an Indiana PII Guidebook for government and the general public by the end of Q1, 2019.

POLICY WORKING GROUP

Deliverable: Policy Research Report

- Objective 1: IECC and partners will develop a report of state and federal cybersecurity legislation by August 2018. *Completed.*

PUBLIC AWARENESS & TRAINING WORKING GROUP

Deliverable: Public Relations Campaign Plan

- Objective 1: The IECC Public Awareness and Training Working Group will complete a statewide public relations cybersecurity campaign plan by June 2018. *Completed.*
- Objective 2: IECC will implement an IECC public relations micro-plan on year-one efforts by September 2018. *Completed.*

STRATEGIC RESOURCE WORKING GROUP

Deliverable: IECC Program Documentation

- Objective 1: IECC will develop program/framework documentation by September 2018. *Completed.*

Deliverable: IECC Scorecard

- Objective 1: IECC, along with Purdue University, will develop Indiana's first Cybersecurity Scorecard by May 2018. *Completed.*
- Objective 2: IECC, along with Purdue University, will launch Indiana's Cybersecurity Scorecard Pilot Program with 90 percent of selected organizations by September 2018. *Completed.*
- Objective 3: IECC, along with Purdue University, will develop a final report of Indiana's Cybersecurity Scorecard Pilot Program by May 2019.

Deliverable: IECC Sustainability Recommendation

- Objective 1: IECC will develop a sustainability recommendation by September 2018. *Completed.*

OBSERVATIONS & CONSIDERATIONS OF IECC

The cybersecurity threat environment is dynamic and complex. Launching a successful statewide cybersecurity strategy is dependent upon a clear and consistent message from leadership at all levels of government. Cybersecurity is a priority for Indiana because of the pervasive threats, which is why the Governor and state lawmakers continue to champion its importance. Defining cybersecurity—and efforts to protect against cybersecurity threats—must be illustrated in a way that is simple yet effective, complete yet attainable. In short, cybersecurity needs to be characterized in a way that eliminates the mystery of what to do next. Effective cybersecurity goes beyond password protections and tip sheets; it requires a shift in the cultural dialogue—moving away from a purely technological view and toward a multi-disciplinary solution to the growing threat. If it is to be effective, these solutions must encompass not only government and businesses at all levels and sizes, but also all Hoosiers across the state. Further, it requires ongoing training programs, continuing public education, toolkits, and updates to address the pervasiveness of cyber threats in today's society. Cybersecurity is an exercise in continuous risk management and will never be a "one-and-done" initiative, nor will it ever offer perfect prevention. Instead, effective cybersecurity is best understood through a lens of evidence-based risk reduction.

As with many important issues, the success of a cybersecurity strategy depends on the resources and funding available to support its implementation. It also is important to note that while these implementation plans have estimated time frames, budgets, and resources, they are agile in nature. The expertise of the members on those committees and working groups will inform updates and necessary corrections to each implementation plan.

It is important that the Council remain aware and prepared to shift focus of deliverables and priorities based on emerging technology and threats. Adapting to a changing threat environment as periodically illustrated by experts and federal partners will be critical to the significant efforts of the Council. The Council will remain flexible to these adaptations but will continue to strive to complete the deliverables laid out in this state plan through the facilitation and assistance of Council leadership.

2018 RECOMMENDATIONS

As many of the deliverables are being implemented, the Council asks that the Governor and his administration continue to support the IECC implementation plans, per the experts of the Council, by:

- Supporting a statewide cybersecurity public relations and awareness campaign designed to nurture fundamental change in culture that will make not only citizens of Indiana safer in their personal endeavors, but also the places they work as good cyber hygiene is presented, understood, and employed over time.
- Encouraging the highest-level technical and administrative cybersecurity best practices and standards as well as support cybersecurity research with a focus on evidence-based policies and practices toward changing behavior and risk reduction.
- Supporting policy that will boost the cybersecurity posture of Indiana. This includes updating 2018 Senate Enrolled Act 362. The current law requires a water or wastewater utility's cybersecurity plan be a public document. An amendment to this law removing the requirement of making the cybersecurity plan a public document, while preserving this requirement for the asset management plan to be public, would ensure the safety of Indiana's critical infrastructure from bad actors.
- Providing necessary support to the critical infrastructures as they move forward with their many deliverables. In particular, utilities such as the water and wastewater where an important tool is being developed to assist operators in evaluating and improving their cybersecurity posture. This also includes efforts such as planning, training, and exercising in preparation of a cyberattack (e.g. working with small critical infrastructure operators in safe environments such as Muscatatuck).
- Encouraging all of Indiana's workforce ecosystem (K-12, post-secondary programs, underemployed, educators, employers, and partners) to follow cybersecurity best practices and national standards such as the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Development Framework; as well as assist in providing resources to educators and businesses in Indiana so that they can best develop and contribute to the cybersecurity talent pipeline.
- Developing the cyber knowledge of law enforcement and emergency management. In particular, law enforcement forensic knowledge so that they are poised to be a part of the Indiana Cybersecurity Emergency Response Team in an event of a cyber emergency.
- Supporting the Council as it moves forward, including ensuring that the Voting and Advisory Members match the needs of the state. This would mean updating the Executive Order to include additional Voting Members representing industries such as transportation, agriculture, advanced manufacturing, and the business community as well as cybersecurity experts, tools, and service providers as the cyber threat continues to evolve.

PART 3
YEAR IN REVIEW

2018 MEMBERSHIP & LEADERSHIP

In 2018, more than 200 members participated in the Council. Of those, Voting and Advisory Members were selected to lead the 20 committees and working groups. For a full list of members and committee working group leadership as of the last membership vote taken by the Council in January 2018, see Appendix E.

BEST PRACTICES OF IECC

The Council has accomplished an unprecedented amount of work for the citizens and businesses of Indiana in the last year due to the commitment of the public, private, military, and academic partnerships. Cybersecurity is not an issue that merely affects information technology professionals but one that affects all Hoosiers and businesses. Taking cybersecurity to the Next Level cannot be done by one entity alone. It is by working collaborally across sectors and areas of expertise to address the comprehensive ecosystem that the state will not only address its own technology and information environment, but also make great strides to further increase Indiana's broader cybersecurity posture.

DELIVERABLES COMPLETED

Each committee and working group was established within the last year, and each began following a four-step strategic process (research, planning, implementation, and evaluation). This process leads Indiana to a comprehensive understanding of the many challenges facing the state, as well as the many current and possible solutions that can enhance cybersecurity at all levels. The Council has identified in detail 69 deliverables to date and, given the right support, those will be implemented over the next few years. In fact, in the first year the Council has completed 27.5 percent of its total deliverables, and 31.6 percent of the 120 objectives.

Some of the deliverables completed within the first year include:

- Statewide cybersecurity general public awareness campaign plan
- Telecommunications sector terminology glossary
- Indiana Office of Defense Development cyber digital platform pilot
- Election system best practices, upgrades, pilot programs, education initiatives, and more
- Energy sector best practices and information
- Indiana's first Cybersecurity Scorecard that will not only provide key indicators to users, but also can be used to directly quantify the effectiveness of the Council
- Professional education pilot program for executives
- Indiana's cybersecurity hub website
- Mechanisms to collect critical infrastructure cybersecurity contact information for the State of Indiana
- Cybersecurity plan template for water and wastewater utilities
- Inventory of cybersecurity sharing resources
- Cybersecurity insurance guide
- Comprehensive cyber policy research including a tool of cybersecurity legislation proposed (passed or failed) in all 50 states and at the federal level since 2011

ADDITIONAL ACCOMPLISHMENTS IN INDIANA

Since the launch of Governor Holcomb's Council Version 2.0 in July 2017, there have been several additional Indiana programs and accomplishments, including:

DEVELOPING THE WORKFORCE

In January 2018, Governor Eric J. Holcomb invited aspiring female high school students to explore their interest in the computer science and technology field by joining the Girls Go *CyberStart* program. *CyberStart* features an online series of challenges that allow students to solve cybersecurity-related puzzles and explore exciting, relevant topics, such as cryptography and digital forensics. More than 100 Indiana teams and 380 young women entered the competition. In the end, 12 Indiana teams made it into the top 100 teams of the nation, and three of those Indiana teams made it into the top 20.

CYBERTECH MIDWEST

The State of Indiana has announced the launch of its first cybersecurity conference, in partnership with Cybertech, to be held on October 23, 2018. Cybertech is a worldwide conference series with events in Tel Aviv, Rome, Singapore, Panama, and other locations. Due to Indiana's collaborative approach to cybersecurity and proven record of public, private, academic, and military collaborations, Indiana secured the conference through 2020. More information at http://midwest.cybertechconference.com/.

CYBER ACADEMY

On August 22, 2018, Governor Holcomb joined officials from the Indiana National Guard and Ivy Tech Community College to cut the ribbon on the new Ivy Tech Cyber Academy. The Cyber Academy, located at the Muscatatuck Urban Training Center, will train military and civilian students in dealing with cyber threats. Students participating in this program can:

- Earn an accelerated Cyber Security/Information Assurance Associate of Applied Science Degree from Ivy Tech Community College - Columbus, an 11-month, 60-credit-hour program.
- Participate in exclusive training and testing events in Muscatatuck's multi-domain environment (land, maritime, air, human and cyberspace), which will provide students opportunities to conduct integrated and synchronized offensive and defensive cyberspace operations.
- Earn highly sought-after, industry-leading certifications useful in both military and civilian careers, including A+, C-CENT and Security+.
- Embark on a career path in government agencies or global security companies including companies right here in Indiana paying an average of more than $70,000 per year by having opportunities to interact with those potential future employers during the program.

JOINING OTHER STATES

The Council re-launch followed Governor Holcomb joining the National Governors Association's (NGA) "A Compact to Improve State Cybersecurity" in mid-July. The 38 governors who signed the compact agreed to protect personal and government data stored on state systems and develop statewide plans to combat cyberattacks waged against information technology networks. The agreement included a pledge to build a cybersecurity governance structure, prepare and defend the state from cybersecurity events, and increase the nation's cybersecurity workforce.

JOINING FEDERAL PARTNERS

In addition to working closely with U.S. Department of Homeland Security (USDHS), Federal Bureau of Investigation (FBI), and other federal partners, IDHS recently signed a Memorandum of Agreement (MOA) with Indiana's Chapter of InfraGard, formalizing the partnership with the State of Indiana. The InfraGard Indiana Members Alliance serves as a link between the public and private organization and is a cooperative undertaking between the U.S. Government (FBI) and an association of local businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the safety/security of Indiana and U.S. critical infrastructures.

JOINING OTHER COUNTRIES

Filing on behalf of the members of the Security in Technology Consortium, the Cyber Leadership Alliance, a non-profit organization that sits on the Council, has been granted membership to Global EPIC. Global EPIC is a worldwide program of cybersecurity ecosystems that includes the U.S., Israel, Canada, the Netherlands, Costa Rica, and others. Academic partners, private companies, and government, including the State of Indiana Chief Information Officer (CIO) and the Cybersecurity Program Director, have joined this consortium and will support projects and research.

NGA CYBER POLICY ACADEMY

As one of four states selected by the National Governors Association Cyber Policy Academy, Indiana will be able to work with other state leaders to share best practices and lessons learned. Knowledge gained from this academy will allow Indiana to accelerate its efforts and increase the knowledge of policies that will enhance education, awareness, response, and protection for all Hoosiers. The Academy also will help to guide a proactive strategy that will address cybersecurity as a common threat and best inform policy discussions that highlight and energize dialogue as the state implements viable, solutions to complex mission areas. Specifically, the state will focus on the Indiana cybersecurity workforce and develop tools for emergency managers for preparing, responding, and recovering from a cyberattack. Furthermore, the Academy will position Indiana to equip other states to implement their own cyber plans and safeguards by creating best practices and solutions that can be implemented across sectors and state lines.

HELPING THE NATION

Indiana is joining other states and providing expertise in addressing cybersecurity issues. By working collaboratively, states can establish long-term protection strategies that will provide other states and their residents with the knowledge and infrastructure they need to feel safer from such threats. Working with other states also will assist Indiana in its development of concrete protocols, policies, and programs of how to best engage and partner with not only the states in the Midwest, but also throughout the nation. This includes cyber threat sharing and response capabilities. Indiana recognizes that cyberattacks do not account for state lines, and state-to-state coordination of support and recovery is necessary when an attack occurs.

IECC MOVING FORWARD

As the Council moves forward with the deliverables in this plan, it is important to note that this is a living document and will be updated regularly. At a minimum, the plan will be updated annually and will include a progress report from each committee and working group to the Governor and public. Moreover, the Council will add committees and working groups in 2019 such as advanced manufacturing, agriculture, transportation, business, and emerging technologies now that the framework has been fully tested and successful. Council membership also will be reviewed and recruitment of experts in the fields will be ongoing.

The goal of the Council is to move cybersecurity to the Next Level in Indiana, but doing so in a way that is as intuitive as possible and does not add more clutter to the already complex topic. Indiana is only as strong as its weakest link. Providing resources to the weakest within the state will not only strengthen the posture of the many organizations who are connected, but also support an infrastructure that will continue to attract businesses and workforce to come to Indiana. With the continued guidance and support of experts throughout the State of Indiana, Hoosiers will be safer and businesses will continue to thrive.

APPENDICES

APPENDIX A

INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY EXECUTIVE ORDER 17-11

STATE OF INDIANA

EXECUTIVE DEPARTMENT
INDIANAPOLIS

EXECUTIVE ORDER **17-11**

FOR: **CONTINUING THE INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY**

TO ALL WHOM THESE PRESENTS MAY COME, GREETINGS.

WHEREAS, the State of Indiana recognizes the critical role that information technology plays in modern society and that state government has a responsibility to support prevention, protection, mitigation, response, and recovery programs related to cyber threats;

WHEREAS, critical infrastructure and key resource sectors rely heavily on information technology to manage complex systems, including, but not limited to, public utility lifelines, healthcare, telecommunications, transportation, financial services, manufacturing, education, research, and public safety;

WHEREAS, cyber threats pose personal, professional, and financial risks to the citizens of the State of Indiana and threaten the security and economy of our State;

WHEREAS, securing Indiana's information technology infrastructure and industrial control systems is beyond the reach of any single entity;

WHEREAS, the diverse authorities, roles, and responsibilities of critical infrastructure stakeholders require a collaborative public-private partnership that encourages unity of effort;

WHEREAS, in order to protect the security and economy of the State, it is appropriate and necessary for state government to establish and lead a statewide, collaborative effort involving government, private-sector, military, research, and academic stakeholders to enhance Indiana's cybersecurity.

NOW, THEREFORE, I, Eric J. Holcomb, by virtue of the authority vested in me as Governor of the State of Indiana, do hereby order that:

1. The Indiana Executive Council on Cybersecurity ("Council") shall be continued.

2. The Council shall be composed of the following Voting Members who shall serve on the Council by virtue of their office or by my appointment and shall serve at my pleasure:

    a. A designated representative of the Governor's Office who shall also serve as the State Cybersecurity Coordinator to administer development and implementation of State cybersecurity strategy and policy.
    b. The Executive Director of the Indiana Department of Homeland Security, or designee.
    c. The Chief Information Officer of the Indiana Office of Technology, or designee.
    d. The Indiana Attorney General, or designee.
    e. The Adjutant General of the Indiana National Guard, or designee.
    f. The Superintendent of the Indiana State Police, or designee.
    g. The Chair of the Indiana Utility Regulatory Commission, or designee.
    h. The Secretary of Commerce of the Indiana Economic Development Corporation, or designee.
    i. The Commissioner of the Indiana Commission for Higher Education, or designee.

j. The Commissioner of the Indiana Department of Revenue, or designee.
k. The Chief Information Officer of Purdue University, or designee.
l. The Chief Information Officer of Indiana University, or designee.
m. One representative of a public interest organization, such as private advocacy or individual information protection.
n. One (1) representative of an association representing the Information Technology Sector.
o. One (1) representative of an association representing the Communications Sector.
p. One (1) representative from an association representing the Defense Industrial Base Sector.
q. One (1) representative from an association representing the Energy Sector.
r. One (1) representative from an association representing the Financial Services Sector.
s. One (1) representative from an association representing the Healthcare & Public Health Sector.
t. One (1) representative from an association representing the Water & Wastewater Systems Sector.

3. The Council will also consist of permanent, non-voting members, as selected by the relevant federal agency:

    a. A cybersecurity expert from the Indianapolis field office of the Federal Bureau of Investigation.
    b. Two (2) cybersecurity experts from the Indianapolis office of the United States Department of Homeland Security, as follows:
        i. One (1) from the Indianapolis office of the United States Department of Homeland Security National Protection and Programs Directorate; and
        ii. One (1) from the Indianapolis office of the United States Secret Service.

4. The Council may also appoint Advisory Members representing both public and private sector interests. Advisory Members shall be selected and approved by a majority of the Voting Members of the Council. The purpose of the Advisory Members is to support Council decision-making by providing subject-matter expertise and specialized insight.

5. The Executive Director of the Indiana Department of Homeland Security, or designee, shall serve as chairperson of the Council.

6. The Council shall establish and maintain a strategic framework document that defines high-level cybersecurity goals for the State. This framework document shall establish a strategic vision for State cybersecurity initiatives and detail how the State will:

    a. Establish an effective governing structure and strategic direction;
    b. Formalize strategic cybersecurity partnerships across the public and private sectors;
    c. Strengthen best practices to protect information technology infrastructure;
    d. Build and maintain robust statewide cyber incident response capabilities;
    e. Establish processes, technology, and facilities to improve cybersecurity statewide;
    f. Leverage business and economic opportunities related to information, critical infrastructure, and network security; and
    g. Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

7. The Council shall develop, maintain and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe.

8. The Council shall receive guidance from the Counter-Terrorism and Security Council and report to the Homeland Security Advisor within the Office of the Governor. All State agencies, departments, commissions, bureaus, institutions, and entities shall cooperate to the fullest extent possible with this Executive Order.

9. The Council shall be staffed by the Indiana Department of Homeland Security.

10. The Council shall be subject to the requirements as well as the security and confidentiality exceptions under the Indiana Open Door Law (Indiana Code § 5-14-1.5) and the Access to Public Records Act (Indiana Code § 5-14-3).

IN TESTIMONY WHEREOF, I,
Eric J. Holcomb, have hereunto set my hand and caused to be affixed the Great Seal of the State of Indiana on this 9th day of January 2017.

Eric J. Holcomb
Governor of Indiana

Connie Lawson

ATTEST: Connie Lawson
Secretary of State

APPENDIX B

INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY CHARTER

Indiana Executive Council on Cybersecurity
Council Charter

Last Updated: September 27, 2017

Version: 4

Table of Contents

ARTICLE 1 – BACKGROUND, NAME & PURPOSE 4
Section I: Background 4
Section II: Name and Purpose 4
ARTICLE 2 – COUNCIL MEMBERS 5
Section I: Council 5
Section II: Classes of Members 6
Chairperson of the Council 6
Council Members 7
Advisory Members 7
Contributing Members 7
Section III: Appointment Terms & Process 8
Section IV: Membership Terms and Requirements 8
Section V: Member Expenses 9
ARTICLE 3 – COUNCIL MEETINGS 9
Section I: Schedule & Process 9
Section II: Announcement of Meetings 9
Section III: Location of Meetings 10
Section IV: Quorum of Members for Meetings 10
Section V: Conduct of Meetings 10
Section VI: Delegation of Authority 11
Section VII: Conflict of Interest 11
ARTICLE 4 – COUNCIL DUTIES 11
Section I: Cyber Projects and Events 11
Section II: Committees and Working Groups 12
Section III: Deadlines 13
Section IV: Document Submissions 13
Sharing and Editing of Documents 13
Repository of Documents 13
Availability of Documents to the Public 13
Council Records 13

Section V: Media Request 13
Section VI: Receipt of Sensitive Information 13
ARTICLE 5 – ADOPTION/AMENDMENT OF COUNCIL CHARTER 14
ARTICLE 6 – NON-EXCLUSION PROVISION 14
ARTICLE 7 – CHARTER ADOPTION & SIGNING 14

ARTICLE 1 – BACKGROUND, NAME & PURPOSE

Section I: Background

Critical infrastructure and key resource sectors rely heavily on information technology to manage complex systems including public utilities, healthcare, telecommunications, transportation, financial services, manufacturing, education, research, and public safety. The reality of interconnectivity is that cyber risks manifest at an unprecedented pace and can pose profound effect on citizens, organizations, and industries and threaten the security and economy of Indiana. This is all the more relevant with the recent worldwide cyber-attacks.

Securing Indiana's information technology infrastructure and industrial control systems is beyond the reach of any single entity. To stay on the forefront of the cyber risk landscape, Indiana has recognized the need to take a forward-thinking approach and design initiatives that leverage whole-of-state assets.

To protect the security and economy of Indiana, Governor Holcomb's Indiana Executive Council on Cybersecurity, which is led by the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana State Police, and the Indiana National Guard, was formed involving government, private-sector, military, research, and academic stakeholders to collaboratively move Indiana's cybersecurity to the Next Level.

Signed by Governor Holcomb on Jan. 9, 2017, the Council was continued through Executive Order 17-11 with the recognition that a cross-sector body of subject-matter experts is required to form an understanding of Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment, especially as it gains more attention from other states, nationally, and internationally.

Section II: Name and Purpose

- The Governor has established the Indiana Executive Council on Cybersecurity (IECC or Council) to lead a statewide, public-private-sector effort to enhance the cybersecurity posture of the State of Indiana and its critical assets.

- The purpose of the Council is to (1) produce an informed overview of Indiana's cyber risks and opportunities; (2) prioritize those items by criticality, and (3) suggest and/or facilitate the implementation of programs/projects designed to achieve associated objectives.

- The Council will provide consultative direction on projects, initiatives, and programs, ensuring whole-of-state needs are met. The Council will confirm that these programs align with the unique needs and risk profiles of critical sectors throughout the state.

- The Council has been designed to accelerate cyber initiatives and ensure Indiana's cyber stakeholders have the resources and support they need to reach the Next level in cyber security.

- Per the Executive Order:
    - The Council shall develop, maintain, and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe.
    - The Council shall establish and maintain a strategic framework document that defines high-level cybersecurity goals for the State of Indiana. This framework document shall establish a strategic vision for Indiana's cybersecurity initiatives and detail how the state will:
        - Establish an effective governing structure and strategic direction;
        - Formalize strategic cybersecurity partnerships across the public and private sectors.
        - Strengthen best practices to protect information technology infrastructure;
        - Build and maintain robust statewide cyber incident response capabilities;
        - Establish processes, technology, and facilities to improve cybersecurity statewide;
        - Leverage business and economic opportunities related to information, critical infrastructure, and network security; and
        - Ensure a robust workforce and talent pipeline in fields involving cybersecurity.
    - The Council shall receive guidance from the Counter-Terrorism and Security Council and report to the Homeland Security Advisor within the Office of the Governor.

ARTICLE 2 – COUNCIL MEMBERS

Section I: Council

Per the Executive Order, the Council shall be composed of the following Voting Members who shall serve on the Council by virtue of their office or by appointment of the governor:

- A designated representative of the Governor's Office who shall also serve as the State Cybersecurity Coordinator to administer development and implementation of State cybersecurity strategy and policy.
- The Executive Director of the Indiana Department of Homeland Security, or designee.
- The Chief Information Officer of the Indiana Office of Technology, or designee.
- The Adjutant General of the Indiana National Guard, or designee.
- The Superintendent of the Indiana State Police, or designee.
- The Indiana Attorney General, or designee.
- The Chair of the Indiana Utility Regulatory Commission or designee.
- The Secretary of Commerce of the Indiana Economic Development Corporation, or designee.
- The Commissioner of the Indiana Commission for Higher Education, or designee.
- The Commissioner of the Indiana Department of Revenue, or designee.
- The Chief Information Officer of Indiana University, or designee.
- The Chief Information Officer of Purdue University, or designee.

- One representative of a public interest organization, such as private advocacy or individual information protection.
- One (1) representative of an association representing the Information Technology Sector.
- One (1) representative of an association representing the Communications Sector.
- One (1) representative from an association representing the Defense Industrial Base Sector.
- One (1) representative from an association representing the Energy Sector.
- One (1) representative from an association representing the Financial Services Sector.
- One (1) representative from an association representing the Healthcare & Public Health Sector.
- One (1) representative from an association representing the Water & Wastewater Systems Sector.

The Council will also consist of permanent, non-voting members, as selected by the relevant federal agency:

- A Cybersecurity expert from the Indianapolis field office of the Federal Bureau of Investigation.
- Two (2) cybersecurity experts from the Indianapolis office of the United States Department of Homeland Security, as follows:
    - One (1) from the Indianapolis office of the United States Department of Homeland Security National Protection and Programs Directorate; and

    - One (1) from the Indianapolis office of the United States Secret Service.

Advisory Members may also be appointed representing both public and private sector interests.

Section II: Classes of Members

Chairperson of the Council

- The Executive Director of the Indiana Department of Homeland Security (or designee) shall serve as **Chairperson of the Council** (the Chair)**.**

- The Chair will work in conjunction with a Core Group consisting of the Chief Information Officer of the Indiana Office of Technology, the Adjutant General of the Indiana National Guard, and the Superintendent of the Indiana State Police to strategically lead the Council.
- The Chair shall supervise and control the business, property and affairs of the Council, except as otherwise provided by law and will have final approval and signatory authority once a majority of the Core Group has approved projects overseen by the Council.

- The Chair and Core Group shall work closely with the Office of the Governor to report on and validate the processes within the Council, and escalate issues as appropriate.

- The State of Indiana may appoint a **Cybersecurity Program Director** to provide both strategy oversight, project management, and logistical support. The Cybersecurity Program

Director will work closely with the Core Group, Governor's Office, and members to meet the objectives set forth by the Executive Order.

Council Members

- **Voting Members** are appointed to voice and reflect the cybersecurity issues of their sector or area of expertise.

- Voting Members may not promote their organization, company or agency over any other in the Council.

- **Non-Voting Members** have equal voice in dialogue, project proposals, and management of items brought forth to the Voting Members of the Council.

- Voting and Non-Voting Members may identify two (2) proxies who may attend meetings and, if applicable, vote on their behalf.

Advisory Members

- Advisory Members may also be appointed representing both public and private sector interests. The purpose of the Advisory Members is to support Council strategy and objectives by providing subject-matter expertise and specialized, experienced insight.

- All private and academic sector Advisory Members must submit their resumes to the Cybersecurity Program Director for vetting. Resumes will be submitted through the Core Group and Governor's Office prior to being provided to the Voting and Non-Voting Members of the Council.

- Advisory Members shall be selected and approved by a majority of the Voting Members of the Council.

Contributing Members

- Pending the approval of becoming an Advisory Member, all subject matter experts will be considered Contributing Members. For long-term expertise, this is only meant as a temporary classification.

- There may be times when the Council is in need of subject-matter experts from other states or countries who provide specialized, limited guidance. These members will be considered Contributing Members.

Section III: Appointment Terms & Process

- Council Members will be appointed by the Office of the Governor for a term of one (1) year. Any representative may serve consecutive terms.

- Council Members will serve at the pleasure of the Governor of Indiana, and may be dismissed at any time.

- Any Voting, Non-Voting, or Advisory Member may be recommended in writing and with reason for removal by majority vote at a regularly scheduled meeting where the item is approved to be placed on the written agenda distributed at least two weeks ahead. The Governor's Office will have final decision-making authority over these recommended removals.

- Critical infrastructure sectors represented on the Council will be based on the most recent assessment of the State's cybersecurity landscape. Sector-specific representation may shift according to changing priorities and risk profiles.

- Council Members are expected to participate in occasional classified security briefings, and must maintain the appropriate status to be granted a temporary clearance.

- Voting, Non-Voting, and Advisory Members are required to maintain good membership standing and meet all the member terms and applicable requirements, or he or she may be removed from the council at any time.

Section IV: Membership Terms and Requirements

- All members are responsible for notifying and seeking approval from their employer to participate on the Council**.**

- All members shall continue to represent their designated organization or sector for the duration of their appointment.

- All state agencies, departments, commissions, bureaus, institutions, and entities shall cooperate to the fullest extent possible with the Executive Order.

- All members (or their proxies if applicable) shall attend at least 75 percent of all scheduled meetings in order to remain in good standing. Members who fail to meet this expectation will be reported to the Chair, Core Group, and Office of the Governor and may be removed from the Council.

- All members who wish to withdraw their membership may do so at any time by submitting a written request to the Chair.

- All members are required to sign and submit a Non-Disclosure Agreement before attending any executive session.

- All members are required to complete Inspector General Ethics Training and applicable forms (e.g. disclosures) in a timely fashion and follow the laws set forth in statute.

- All members shall do their best to avoid any look of impropriety regarding their membership and the Council.

- All private sector members are required to be an InfraGard member and must submit timely proof of membership.

- All public and academic members are strongly encouraged to be an InfraGard member. If he or she is a member, membership proof is required to be submitted.

- All members must have access and agree to use the software platform for central repository and project management selected for the Council by the Cybersecurity Program Director.

- All members must serve in a capacity in at least one of the committees or working groups.

- All members will be required to complete a *Committee and Work Group Form* and submit it to the Cybersecurity Program Director for consideration.

- All members must comply with the charters and guidelines set forth by the Council, committees, and/or working groups in which they are involved.

Section V: Member Expenses

- Participation in the Council is entirely voluntary, and expenses for travel, per diem, etc. will not be remunerated at this time.

ARTICLE 3 – COUNCIL MEETINGS

Section I: Schedule & Process

- The Council Meeting schedule and agendas are collectively set by the Chair, Core Group, Governor's Office, and Cybersecurity Program Director.

- Meetings shall generally be held on a quarterly basis or as needed per the strategic plan deadlines and approvals.

- A special or emergency Council meeting may be called in the case of pertaining events. This may be done at the suggestion of a Council Member(s) or the Chair at a permitting facility.

Section II: Announcement of Meetings

- The Council shall be subject to the requirements as well as the security and confidentiality exceptions under the Indiana Open Door Law, per the Executive Order.

- Members will be notified at each meeting of the next meeting time, place, and date, and will be notified in writing at least four weeks in advance of such meetings with a verified date, time, and

place. All materials subject to vote and a draft agenda will be provided to Voting and Non-Voting Members at least two weeks prior to the scheduled meeting.

- The public will be notified of Council meetings by notices issued by the Indiana Department of Homeland Security, in the manner prescribed by law.

- Executive sessions exclusive to Council Members may be scheduled at the discretion of the Chair or designee.

- The Council herby adopts a policy so that the committees and working groups may conduct meetings using means of electronic communication per IC 5-14-1.5-3.6.

Section III: Location of Meetings

- Council meetings shall be held in the Indiana Government Center's Conference Center, 302 West Washington Street, Indianapolis, Indiana 46204, or as otherwise determined by the Chair.

- Exceptions may be permitted for off-site meetings at the suggestion of Council Member(s) and at the discretion of the Chair.

- Attending meetings by conference call or Internet usage is prohibited. Council Members who cannot attend may have a proxy attend in their stead.

Section IV: Quorum of Members for Meetings

- A quorum of 85 percent of the Voting and Non-Voting Council Members is required for the conduct of business and consists of the presence of a majority of its members.

Section V: Conduct of Meetings

- Council meetings will be conducted according to Robert's Rules of Order, and Council business according to the provisions of the Indiana Open Door Law, the Indiana Public Records Law, and the Indiana Administrative Orders and Procedures Act.

- A vote may be held to approve Council activities or statewide strategic projects, documents, and requests to the Governor's Office or General Assembly.

- Any matter to be voted on will take the form of a resolution or motion. A simple majority of the Voting Members in attendance at a Council meeting must vote affirmatively, for the adoption of any resolution.

- Each Voting Member will have one vote.

- A Council Member may vote for or against a resolution, or may abstain from voting.

- All Voting Members of the Council shall have equal voting rights.

- Votes must be cast in person. Council Members who cannot attend may have one of their pre-approved proxies vote on their behalf.

Section VI: Delegation of Authority

- In the absence of the Director, Council meetings will be conducted by the Cybersecurity Program Director or Chair's designee.

- The Council Chair may delegate in writing at his discretion his powers and duties consistent with other provisions of the Charter.

- Each Council Member may provide in writing up to two (2) designees with full voting rights to represent such organizational head in his/her absence from Council meetings.

Section VII: Conflict of Interest

- Whenever a Voting Member has a financial interest in a matter coming before the Council, the person shall a.) fully disclose the nature of the interest and b.) withdraw from a voting process.

- The meeting minutes at which such votes are taken shall record such disclosure, abstention and rationale for approval.

ARTICLE 4 – COUNCIL DUTIES

Section I: Cyber Projects and Events

- Council Members representing state departments/agencies are expected to leverage the expertise provided by the Council and submit statewide, cross-sector, or significant cybersecurity projects and/or events to the Council for review and input, except in instances in which doing so would be in violation of law or policy, or in which doing so could jeopardize the event or project.

- Council Members representing the private and academic sector are strongly encouraged to leverage the expertise provided by the Council and request the participation or feedback of all Council Members on statewide or cross-sector cybersecurity projects and/or events.

- In an effort to cross-promote cyber events in Indiana, members are encouraged to submit cyber events to the Cybersecurity Program Director to list on www.in.gov/cybersecurity at least six weeks prior to the event. Once a month, a notification will be sent to subscribers and all Council members.

- Agency heads or project managers may submit their project proposals to the Cybersecurity Program Director at least six weeks before the requested meeting date.

- Council Members may suggest changes to project content submitted to the Council based on their subject-matter expertise; suggestions will be non-binding unless the matter requested to be escalated to a vote by the responsible agency head or project manager.

Section II: Committees and Working Groups

- All members must serve in a capacity in at least one of the committees or working groups:
    - Government Service Committee
    - Finance Committee
    - Energy Committee
    - Water and Wastewater Committee
    - Communications Committee
    - Healthcare Committee
    - Defense Industrial Committee
    - Elections Committee
    - Economic Development Committee
    - Workforce Development Committee
    - Personal Identifiable Information Working Group
    - Public Awareness and Training Working Group
    - Emergency Services and Exercise Working Group
    - Cyber Sharing Working Group
    - Policy Working Group
    - Cyber Pre- and Post- Incident Working Group
    - Legal and Insurance Working Group
    - Local Government Working Group
    - Strategic Resource Working Group

- All members must comply with the charters and guidelines set forth by the Council, committees, and/or working groups in which they are involved.

- Membership of each committee and workgroup consist of:
    - Chairs
    - Co-Chairs
    - Full-time Members
    - As-needed Members
    - Contributing Members (Transition only between voting of Advisory Members)

- All members will be required to complete a *Committee and Work Group Form* and submit it to the Cybersecurity Program Director. Choices will be strongly considered, but not guaranteed. No one person can participate in more than three committees or working groups. This is to ensure that all committees and working groups are as cross-functional and diverse in its expertise as possible.

- All Committee and Working Groups will provide the Cybersecurity Program Director an update the first Friday of every month reporting on the month before, per the details of the committee's charter or working group guidelines.

Section III: Deadlines

All members of the Council shall meet all established deadlines of items for review, deliverables, and strategy. If a deadline will not be met, member is responsible for notifying the Cybersecurity Program Director with the reason why the deadline will be missed and the expected completion date.

Section IV: Document Submissions

Sharing and Editing of Documents

- For the purposes of the electronic file sharing and a central repository, all members will be required to sign up and use Syncplicity (https://www.syncplicity.com/register/personal). If a member is a State of Indiana employee, he or she will receive an email from the Indiana Office of Technology to set up their state account. Once signed up, each member will be invited by the Cybersecurity Program Director to join his or her relative folders.

Repository of Documents

- The Indiana Department of Homeland Security (IDHS), 302 West Washington Street, Room E238, Indianapolis, Indiana 46204 will be the repository for all documents submitted to the Council pursuant to the provisions of federal or state law.

Availability of Documents to the Public

- Public records will be available for examination by the public during the hours of 8:30 am and 4:30 pm, Monday through Friday.

Council Records

- All records of general meetings, including meeting agendas and minutes, will be available for inspection and copying by any person at 302 West Washington Street, Room E238, Indianapolis, Indiana 46204.

Section V: Media Request

- If a member is contacted by the media for an issue related to the IECC, please direct them to the IDHS Office of Public Affairs at PIO@dhs.in.gov or 317-234-6713.

Section VI: Receipt of Sensitive Information

- The Council may receive sensitive security information from the Indiana Department of Homeland Security, Indiana Office of Technology, or the Indiana Army National Guard. This information shall remain for official use only, and Council Members are expected to abide by handling instructions.

- The Council may receive sensitive law enforcement information from the State Police Department, the Federal Bureau of Investigation, or other federal, state, or local law enforcement agencies. This information shall not be released to the news media or others without a need to know.
- Council Members who release such information to external parties without prior approval are subject to immediate dismissal from the Council.

ARTICLE 5 – ADOPTION/AMENDMENT OF COUNCIL CHARTER

- A majority of Council Members is required to adopt the Council's Charter.
- Once approved, the Council Charter will be reviewed every year.
- The Charter may be amended by majority vote at a regularly scheduled Council meeting.

ARTICLE 6 – NON-EXCLUSION PROVISION

- Nothing in this Charter is to be construed as excluding or contravening any additional provisions of federal or state law that are not explicitly or implicitly referred to within this Charter.

ARTICLE 7 – CHARTER ADOPTION & SIGNING

Upon their adoption by the Council, a copy of this Charter will be signed and dated by the Chair, Core Group, and the Cybersecurity Program Director of the Council and will be available for inspection by the public at 302 W. Washington Street, Room E238, Indianapolis, Indiana.

APPENDIX C

INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY PHASE FORMS

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

COMMITTEE AND WORKING GROUP QUESTIONNAIRE – RESEARCH PHASE 1

Instructions: As your committee or working group is in the Research Phase, it is important we work with other committees and working groups to get the information your team will need to be successful. Please answer the questions the best you can.

Provide your questions and answers to MosleyCLM@iot.in.gov.

Committee/Working Group Completing Questions: _____

Person Submitting Answers: _____

Email of Person Submitting: _____

Date Submitted: _____

1. What has your area done in the last five years to educate, train, and prepare for cybersecurity?
2. What (or who) are the most significant cyber vulnerabilities in your area?
3. What is your area's greatest cybersecurity need and/or gap?
4. What federal, state, or local cyber regulations is your area beholden to currently?
5. What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?
6. What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.
7. What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?
8. What does success look like for your area in one year, three years, and five years?
9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?
10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?
11. What do we need to do to attract cyber companies to Indiana?
12. What are your communication protocols in a cyber emergency?
13. What best practices should be used across the sectors in Indiana? Please collect and document.

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

COMMITTEE AND WORKING GROUP: RESEARCH EXECUTIVE SUMMARY TEMPLATE
PHASE 1

Committee/Working Group: _____

Person Submitting Summary: _____

Email of Person Submitting: _____

Date Submitted: _____

Executive Summary

- **Research Conducted**

- **Research Findings**

- **Preliminary Deliverables**

- **Additional Notes**

- **References**

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

COMMITTEE AND WORKING GROUP QUESTIONNAIRE – PLANNING PHASE 2

Instructions: As your committee or working group is in the Planning Phase, it is important we work with other committees and working groups to get the information your team will need to be successful. Below are all the committees and working groups' questions submitted by other teams. Please answer the questions the best you can. If it does not apply to your group, write in N/A. If the answer to a question is confidential/sensitive, please write the reason as to why it cannot be shared in this questionnaire. Do not leave questions with no answer.

Provide your questions and answers to MosleyCLM@iot.in.gov.

Committee/Working Group Completing Questions: _____

Person Submitting Answers: _____

Email of Person Submitting: _____

Date Submitted: _____

Government Service Committee

- Do you know of other state level cyber plans?
- How do state entities interface with existing national groups? The energy industry currently works with two national cyber coordinating councils (one for electric industry and one of the natural gas industry.) These groups include U.S. Department of Homeland Security personnel.
- What federal agencies have cybersecurity services/functions? What services do they provide?
- What communications following an incident would you like from energy utilities?
- How will state and federal agencies allocate scarce resources in an emergency? For example, fuel to allow back-up generators to operate.
- What do you expect to receive from the Committee/Working Groups?
- Which Committee/Working Groups do you expect to be most involved with during the implantation of your deliverables?
- What does your team expect from the (critical infrastructure) CI sectors during incident response?
- How does your sector currently coordinate and collaborate with each CI sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)

- Do you know of or participate in joint sector cyber exercises?
- How can we best institute joint-purchasing or sharing of government resources to protect infrastructure?
- How can local governments access the necessary infrastructure (i.e. to fiber optics) that are needed to provide adequate back-up systems and necessary redundancies?
- How can government use volunteers who are experts in the field versus paying for a vendor that provides the same service?
- What does Government Services uses for 3rd Party vendor assessment questions?
- What does Government Services follow Security Framework?
- Is there a Knowledge center to share information without recourse?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- How are cyber incident emergencies managed in your CI sector and who do you contact for incident response?
- What exercise planning and management support can US-CERT and ICS-CERT provide to local government, state government, and private sector?
- What existing state agency services are available for individual, small-business, and local government cyber-crime response?
- What processes are in place for information sharing between and within CI sectors?
- How often are cybersecurity plans exercised and evaluated?
- What cyber incident response capabilities does the state currently support for recovery from a cyber event?
- Do state agencies carry insurance for cybersecurity risks, such as data breaches, cyber extortion, and other privacy breaches? If so, provide details regarding the insurance policies that apply to such risks. For example, are they endorsement or customized stand-alone policies? Who is the insurer and does the policy offer the following coverages: network and information security liability, communications and media liability, regulatory defense expenses, crisis management event expenses, security breach remediation and notification expenses, computer fraud, funds transfer fraud, e-commerce extortion, business interruption. (Provide sample policy/endorsements.)
- Do state agencies have a standard cybersecurity agreement with outside vendors that have access to data? Or does the language of the agreement vary per agency? If so, do those agreements require such vendors to carry insurance for cybersecurity risks? (Provide sample cop(ies) of agreement(s).)
- Do state agencies carry insurance for cybersecurity risks, such as data breaches, cyber extortion, and other privacy breaches? If so, provide details regarding the insurance policies that apply to such risks. For example, are they endorsement or customized stand-alone policies? Who is the insurer and does the policy offer the following coverages: network and information security

liability, communications and media liability, regulatory defense expenses, crisis management event expenses, security breach remediation and notification expenses, computer fraud, funds transfer fraud, e-commerce extortion, business interruption. (Provide sample policy/endorsements.)

- Do state agencies have a standard cybersecurity agreement with outside vendors that have access to data? Or does the language of the agreement vary per agency? If so, do those agreements require such vendors to carry insurance for cybersecurity risks? (Provide sample cop(ies) of agreement(s).)
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Finance Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How can local governments fund cyber protection once it is determined what measures should be put in place?
- What are the minimum amounts that should be budgeted for cyber protection?
- Are there any collaborations that are possible to share the cost of funding?
- What does Finance sector use for 3rd Party vendor assessment questions?
- What does Finance sectors follow Security Framework?
- FFIEC - does anyone use FFIEC criteria and guidance to what extent?
- Any guidelines for Small Finance businesses or HealthCare sector?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What are the funding options for state level departments to obtain cybersecurity insurance?
- Is there current funding, assistance, or pooling in place for local entities, including schools and county clerks, to obtain cybersecurity insurance? If not, does the state have other options to assist local entities to pay for cybersecurity insurance?
- What are the funding options for state level departments to obtain cybersecurity insurance?
- Is there current funding, assistance, or pooling in place for local entities, including schools and county clerks, to obtain cybersecurity insurance? If not, does the state have other options to assist local entities to pay for cybersecurity insurance?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Energy Committee

- What do you expect to receive from the Committee/Working Groups?
- What information about cybersecurity posture is collected or surveyed of the sector (required or voluntarily) and by whom?
- How is Protected Critical Infrastructure Information (PCII) maintained by the collecting agency when sharing compiled information?
- What does Energy sector use for 3rd Party vendor assessment questions?
- What does Energy sector follow Security Framework?
- Where does HealthCare fall in the order of delivering service after a disaster?
- Does the sector have a good contact list for local Healthcare officials?
- Any regulations preventing HealthCare standing up Solar or wind?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Water and Wastewater Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How do we design water and waste water cyber security protections for treatment plants with varying levels of connectivity?
- What does Water/Wastewater sector use for 3rd Party vendor assessment questions?
- What does Water/Wastewater sector follow Security Framework?
- Where does HealthCare fall in the order of delivering service after a disaster?
- Does the sector have a good contact list for Local Healthcare officials?
- Are there regulations on using Groundwater?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- How are cyber incident emergencies managed in your CIKR sector and who do you contact for incident response?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Communications Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- If the telecommunications network is interrupted, what back-up or alternatives are available to assist energy companies in maintaining safe operations?
- How can local government best protect our emergency response communication systems?
- What does Communications sector use for 3rd Party vendor assessment questions?
- What does Communications sector follow Security Framework?
- Where does HEALTHCARE fall in the order of delivering service after a disaster?
- Does the sector have a good contact list for Local Healthcare officials?
- Are there Communication channels for disasters
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Healthcare Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- What information about cybersecurity posture is collected or surveyed of the sector (required or voluntarily) and by whom?
- How is Protected Critical Infrastructure Information (PCII) maintained by the collecting agency when sharing compiled information?
- Does anyone have the ability or support Wells?
- What types of Cyber Tabletop formats have you performed?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Defense Industrial Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- What does Defense sector use for 3rd Party vendor assessment questions?
- What does Defense sector follow Security Framework?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- Are there uniform security standards and/or cyber insurance requirements for each election district?

Elections Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- What does Elections use for 3rd Party vendor assessment questions?
- What does Elections follow Security Framework?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- Are there uniform security standards and/or cyber insurance requirements for each election district?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Economic Development Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- Is there software to electronically "sort" the vast amount of data to help identify and prioritize risks?
- Has anyone created a centralized clearinghouse which assesses vendors with differing levels of cybersecurity exposure and risk mitigation?
- Is there a centralized way to understand the risks in a particular component right "out of the box" when a utility procures that component? This should include things like chain of custody for the component or who built a subcomponent.
- What other policy changes could encourage sector growth?
- What would impact be of eliminating non-competes? What if non-compete exclusion only applied if individual left to start new business (competing, but not leveraging IP)?
- Should there be a cyber investment credit for businesses? If they use Indiana-based companies? How to offset investment by Small/Medium Businesses?
- How do we ensure infrastructure is in place?
- Once a sector can quantify moving their Cybersecurity how can we use that to bring more development
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Workforce Development Committee

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- Training of skilled cybersecurity professionals, including those with less that a four-year degree. The NIST National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework, developed in August 2017, provides the foundational skills necessary in various roles within the cybersecurity protection departments of Indiana's energy companies. Is this the model every sector should be following?
- Once a sector can quantify moving their Cybersecurity how can we use that to bring more development?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison
- with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- What are the current STEM education and outreach initiatives within the state?
- Are there cyber tax credits/Tuition reimbursement programs?
- Are there Federal grants?

Personal Identifiable Information Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- Local governments house sensitive personal identification information from citizens (i.e. social security numbers, child protection records, etc.) – how can we best protect it?
- Local governments house data that is public information (such as property records, arrest records, election information, and historical financial information). Although accessible to the public, a loss of these records would be devastating to the operation of government. How do we best protect it?
- How will information about Critical Infrastructure companies, and key employees be managed?
- What Risk and process assessments should local government use to protect their data?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- Has anyone considered expanding the definition to include biometric information, unencrypted login and password combinations, html5 "digital fingerprint," unencrypted knowledge-based authentication questions, unique policy numbers, unique account numbers, debit card numbers where the card may be used as a credit card?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- How are cyber incident emergencies managed in your CIKR sector and who do you contact for incident response?

Public Awareness and Training Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How do we train local government employees to institute cyber security protections?
- What should the training curriculum be?
- Are there way to collaborate to standardize training and share training costs between governmental entities?
- What training support will be available to each of the verticals?
- What has worked in the past for driving public education and messages?
- How can we align to help drive public awareness for the sectors?
- What mechanisms are you planning on using to distribute any training materials created by the Council?
- Are you concentrating on both the public and private sectors?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as a liaison with other committee/working groups?
- How can we all identify, differentiate, and clarify cyber terminology: cyber, cybersecurity, cyber incident, cyber emergency, etc.?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- What programs, if any, currently focus on public awareness and training for any state function?

Emergency Services and Exercise Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How can local government best protect our emergency response communication systems?
- How does HEALTHCARE notify Emergency Service for issues / diverting patients?
- Planned for Cyber-attacks for the sector? If done, what were the results of the exercise?
- What are Cyber Tabletop formats and strategies used?
- Are there knowledge center to share information without recourse?
- Do you have sample table top exercises?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- What programs, if any, currently focus on public awareness and training for any state function?

Cyber Sharing Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- What legitimate cyber protection tools are already available to local government to guard against cyber threats?
- Is IN-ISAC used as an information sharing method?
- Is there a place for Knowledge center to share information without recourse?
- How are we going to promote a culture of cyber sharing within the state in such a way to provide no recourse/retribution for those People/Entities who share cyber-related information?
- How do you intend to share threat intelligence to organizations that don't have the ability to process stix feeds, etc?
- Do you have information about the best way to receive and respond to cyber threat information?
- Training materials for this?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Policy Working Group

- What do you expect to receive from the Energy Committee?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- There is a need to strengthen communications between the sectors. For example it is not unprecedented that an issue in the financial sector appears in the Energy sector later. How can this be accomplished?
- Any regulations preventing HEALTHCARE standing up Solar or wind?
- Any Regulations preventing HEALTHCARE from sanding up direct wells?
- Sample policies for physical security of systems?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?

Pre thru Post Incident Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- What should local governments be doing pre-incident to make sure that internal controls are in place?
- What is the best approach for local governments to institute penetration testing?
- What is the best approach for local governments to use for cyber security planning, response and recovery?
- Contact info to obtain services as needed?
- When or how to use 'jump team'?
- Sample Incident response plans?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Legal and Cyber Insurance Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- Can the state offer a statewide insurance policy that is available to local governments in order to provide a cost-savings?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Local Government Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How is cybersecurity for water/wastewater managed?
- How does the local government work with the local HealthCare system?
- Is there current funding, assistance, or pooling in place for local entities, including schools and county clerks, to obtain cybersecurity insurance? If not, does the state have other options to assist local entities to pay for cybersecurity insurance?
- Are there current guidelines for local entities and school systems regarding cybersecurity insurance for the local entities and for outside vendors that handle private electronic data?
- Do we know how many local governments carry insurance for cybersecurity risks, such as data breaches, cyber extortion, and other privacy breaches? If so, provide details regarding the insurance policies that apply to such risks. For example, are they endorsements or stand-alone customized policies? Who is the insurer and does the policy offer the following coverages: network and information security liability, communications and media liability, regulatory defense expenses, crisis management event expenses, security breach remediation and notification expenses, computer fraud, funds transfer fraud, e-commerce extortion, business interruption. (Provide sample policy/endorsements.)
- Is there current funding, assistance, or pooling in place for local entities, including schools and county clerks, to obtain cybersecurity insurance? If not, does the state have other options to assist local entities to pay for cybersecurity insurance?
- Are there current guidelines for local entities and school systems regarding cybersecurity insurance for the local entities and for outside vendors that handle private electronic data?
- Do we know how many local governments carry insurance for cybersecurity risks, such as data breaches, cyber extortion, and other privacy breaches? If so, provide details regarding the insurance policies that apply to such risks. For example, are they endorsements or stand-alone customized policies? Who is the insurer and does the policy offer the following coverages: network and information security liability, communications and media liability, regulatory defense expenses, crisis management event expenses, security breach remediation and notification expenses, computer fraud, funds transfer fraud, e-commerce extortion, business interruption. (Provide sample policy/endorsements.)
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).
- Who/what are your audiences that need to be reached?

- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?

Strategic Resource Working Group

- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How do local governments choose a legitimate/reputable provider of cyber security services?
- How do local governments differentiate between vendors that are vying for business?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- How can cybersecurity information collected for surveys, assessments, and evaluations of water/wastewater entities be shared with the state?
- Who can help at the state level make a more formal request?
- How can we identify, differentiate, and clarify terminology: cyber, cybersecurity, cyber incident, cyber emergency, etc.?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

Cyber Summit Working Group

- What other cyber conferences/summits are held in the USA and internationally?
- What do you expect to receive from the Committee/Working Groups?
- What does your Sector expect from the Energy sector during incident response?
- How does your sector currently coordinate and collaborate with the energy sector?
- Which electric or natural gas energy services does your sector utilize?
- Does your sector provide its own energy (e.g., solar, microgrid, hydro, etc.)?
- Do you know of or participate in joint sector cyber exercises?
- Do you know of other state level cyber plans?
- What communications following an incident would you like from energy utilities?
- How do local governments choose a legitimate/reputable provider of cyber security services?
- How do local governments differentiate between vendors that are vying for business?
- Who/what are your audiences that need to be reached?
- What current means of communications with these audiences are available or in use in your industry?
- What key messages need to be shared?
- Which of those messages should only go to certain audiences?
- What training for your audiences needs to be provided?
- As we move forward working with you, who should serve as our liaison with your committee/working group for the Public Awareness and Training Group?
- How can cybersecurity information collected for surveys, assessments, and evaluations of w/ww entities be shared with the state? Who can help at the state level make a more formal request?
- Can this summit be used to identify, differentiate, and clarify terminology: cyber, cybersecurity, cyber incident, cyber emergency, etc.?
- What laws or regulations (state or federal) impact your organization's cybersecurity initiatives?
- Please identify any positive effects of these laws/regulations on your organization (identifying which laws in particular).
- Please identity any negative effects of these laws/regulations on your organization (identifying which laws in particular).

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

DELIVERABLE FORM
PHASE 2

IECC Committee/Working Group: _____
Person Submitting Form: _____
Date: _____

PHASE 2 – PLANNING

1. What is the deliverable?

2. What is the status of this deliverable?
   ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

3. Which of the following IECC goals does this deliverable meet? Check **ONE** that most closely aligns. See Executive Order 17-11 for further context.

   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. Which of the following categories most closely aligns with this deliverable (check **ONE**)?
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable:

5. What is the resulting action or modified behavior of this deliverable?

6. What metric or measurement will be used to define success?

7. What year will the deliverable be completed?
   ☐ 2018 ☐ 2019 ☐ 2020 ☐ 2021 ☐ 2022 ☐ 2023+

8. Who or what entities will benefit from the deliverable?

9. Which state or federal resources or programs overlap with this deliverable?

Additional Questions:

10. What other committees and/or working groups will your team be working with to complete or plan this deliverable?

11. Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?

12. Who should be main lead of this deliverable?

13. What are the expected challenges to completing this deliverable?

PHASE 3 – IMPLEMENTATION

As your team works through completing the Deliverable Form for Phase 2, please begin making note and thinking through the specific tasks, owners, and deadlines to complete this deliverable. In addition, start discussing the estimated budget to start the deliverable, budget to sustain the deliverable (if applicable), resources (staff, structure, stuff), etc. Further direction will be provided in the coming weeks for Phase 3.

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

IMPLEMENTATION PLANNING FORM
PHASE 3

IECC Committee/Working Group:
Person Submitting Form:
Date:

PHASE 3 – IMPLEMENTATION PLANNING

1. What is the deliverable?

2. Is this a one-time deliverable or one that will require sustainability?
   ☐ One-time deliverable
   ☐ Ongoing/sustained effort

Tactic Timeline (Please add rows as needed.)

Tactic	Owner	% Complete	Deadline	Notes

Resources and Budget

3. Will staff be required to complete this deliverable? ☐No ☐ Yes
   a. If Yes, please complete the following:

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes

4. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes

Benefits and Risks

5. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

6. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

7. What is the risk or cost of not completing this deliverable?

8. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

9. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics? ☐No ☐ Yes
   a. If Yes, please list states/jurisdictions: Click or tap here to enter text.

10. Are there comparable jurisdictions (e.g. other states) that **does not** have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable? ☐No ☐ Yes
    a. If Yes, please list states/jurisdictions: Click or tap here to enter text.

Other

11. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

12. Does this deliverable require a change from a regulatory/policy standpoint? ☐No ☐ Yes
    a. If Yes, what is the change and what could be the fiscal impact if the change is made?

13. What will it take to support this deliverable if it requires ongoing sustainability?

14. Who has the committee/working group contacted regarding implementing this deliverable?

15. Can this deliverable be used by other sectors? ☐No ☐ Yes,
    a. If Yes, please list sectors:

Communications

16. Once completed, which stakeholders need to be informed about the deliverable?

17. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)? ☐No ☐ Yes

18. What are other public relations and/or marketing considerations to be noted?

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

EVALUATION FORM
PHASE 4

IECC Committee/Working Group:
Date:

PHASE 4 – EVALUATION PHASE

Deliverable:

Objective 1:

Type: ☐ Output ☐ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2:

Type: ☐ Output ☐ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Evaluative Methods Details for all methods except "Completion"

#	Who	How	Owner	Staff #	Costs	Funding Source	Schedule / Frequency	Notes
1								
2								
3								
4								
5								

Questions

Notes

APPENDIX D

INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY COMMITTEE & WORKING GROUP IMPLEMENTATION PLANS

APPENDIX D.1
COMMUNICATIONS COMMITTEE

COMMUNICATIONS COMMITTEE STRATEGIC PLAN

Chair: Joni Hart | Co-Chair: Dan Solero

September 2018
Indiana Executive Council on Cybersecurity

Communications Committee Plan

Contents

Committee Members **4**
Introduction **6**
Executive Summary **8**
Research **11**
Deliverable: Voluntary Industry Contact List **19**
General Information 19
Implementation Plan 20
Evaluation Methodology 23
Deliverable: Communications Sector Terminology Glossary **25**
General Information 25
Implementation Plan 26
Evaluation Methodology 30
Deliverable: Communications Sector Whitepaper **32**
General Information 32
Implementation Plan 33
Evaluation Methodology 37
Deliverable: Cyber Incident Response Engagement Guidance **39**
General Information 39
Implementation Plan 40
Evaluation Methodology 44
Supporting Documentation **46**
Telecommunication Terms 47

Committee Members

Committee Members

Name	Organization	Committee Position	IECC Member Type
Joni K. Hart	Broadband Innovation Group	Chair	Voting
Daniel J. Solero	AT&T	Co-Chair	Voting Proxy
John Greene	New Lisbon Telephone Company	Full time	Advisory
James Haley	City of Fort Wayne	Full time	Advisory
Benjamin Marrero	Ivy Tech Community College	As needed	Advisory
Barry Ritter	Indiana Statewide 911 Board	Full time	Advisory
Rami Mohamad Salahieh	Ivy Tech	As needed	Advisory
David Vice	Integrated Public Safety Commission	Full time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Definition: Determine how various stakeholders and organizations define the Communications Sector nationally and locally.
  - Relationships: Determine key relationships between public and private sector stakeholders driven by existing frameworks, such as National Security Telecommunications Advisory Committee (NSTAC), National Coordinating Center for Communications (NCCC), Department of Homeland Security (DHS), and private sector initiatives.
  - Responsibilities: Determine what rules and practices govern the cybersecurity activities of sector stakeholders and players in terms of regulation, legislation, and accepted best practices.
  - Cross-Sector Planning: Determine what unique characteristics of the Communications Sector environment present opportunities for better cross-sector planning and understanding.
  - Opportunities: Determine what threats, market opportunities and technology advancements are driving cyber security activities in the communications sector.

- **Research Findings**
  - Definition: The sector is generally accepted to be consistent with the definitions used at the Federal level by organizations such as the Department of Homeland Security (DHS) and the National Security Telecommunications Advisory Committee (NSTAC).
  - Relationships: Sector members in the private sector partner on many public policy issues through organizations such as the Broadband Innovation Group, the Indiana Broadcasters Association (IBA), the Indiana Broadband and Technology Association (IBTA), National Security Telecommunications Advisory Committee (NSTAC), the Communications Information Sharing and Analysis Center (known as NCC), and similar cross-industry associations and government-sponsored bodies.
  - Responsibilities: The Communications Sector features a diverse landscape of regulatory and legislative responsibilities at all levels (local, State, National, and International). At the State level, the Indiana Utility Regulatory Commission (IURC) provides regulatory oversight to a vast swath of the Communications Sector. At the Federal level, the Federal Communications Commission provides similar oversight. Cybersecurity responsibilities are additionally stipulated through a matrix of Federal and State bodies as authorized by State and Federal law. Across all sectors, the US-CERT National Cyber Incident Response Plan lays out many key roles and responsibilities that map into a broader Federal response framework.
  - Cross-Sector Planning: Many stakeholders in the Communications Sector operate both at the national and international levels. These organizations are afforded opportunities to participate directly in industry and government associations like National Security Strategy (NSS), NSTAC, and various related organizations. Sector members who operate more locally within the State may benefit from a more cohesive partnership coordinated through the Multi-State Information Sharing and Analysis Center (MS-ISAC).

- Opportunities: Information sharing continues to drive much of the cybersecurity coordinated planning across the sector and with other industry and public stakeholders. Specific technology-driven innovations that enable a faster response may offer opportunities to deepen these partnerships and drive to a more cohesive and effective partnership architecture.

- **Committee Deliverables**
  - Communications Sector White Paper
  - Cyber Contact Lists
  - Cyber Incident Response Engagement Guidance

- **References**
  - DHS Critical Infrastructure Sector-specific Overview: https://www.dhs.gov/communications-sector
  - DHS 2015 Sector-specific Plan: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf
  - National Council of ISACs: https://www.nationalisacs.org/member-isacs
  - Burning Glass Technologies: http://burning-glass.com
  - US-CERT National Cyber Incident Response Plan: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
  - Multi-State ISAC (MS-ISAC): https://www.cisecurity.org/ms-isac/
  - National Security Telecommunications Advisory Committee (NSTAC): https://www.dhs.gov/national-security-telecommunications-advisory-committee
  - Indiana Office of Utility Consumer Counselor: http://www.in.gov/oucc/2492.htm
  - National Center for Systems Security and Information Assurance (CSSIA): http://www.cssia.org/
  - CyberSeek.org: http://cyberseek.org/heatmap.html
  - Indiana Utility Regulatory Commission: http://www.in.gov/iurc/
  - Federal Communications Commission: http://www.fcc.gov
  - Broadband Innovation Group: http://broadbandig.org/
  - Indiana Broadcasters Association: https://www.indianabroadcasters.org/

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. The communications sector has been at the forefront of cybersecurity research, innovation, response planning, and cross-industry coordination. Industry companies participate in many DHS charter organizations, such as the Communications Sector Coordinating Council, where 35 communications sector companies work in partnership with DHS to define priorities and protection objectives for National Critical Infrastructure. Similarly, the Communications ISAC (NCC) and the National Security Telecommunications Advisory Committee (NSTAC) feature robust public/private partnerships aimed at furthering the National strategic approach to protecting critical infrastructure relates to the communications sector.
    b. Private companies in the communications sector compete for cybersecurity workforce resources with all other sectors. Talent shortages continue to drive innovative approaches to continuing education and skillset pivots in the existing workforce. Many organizations encourage and share cost for college degree programs in computer science and cybersecurity. AT&T, as an example, has taken the additional steps of developing robust internal certification curriculums in order to organically grow a market-competitive workforce.
    c. Additionally, communications sector companies invest in cybersecurity research programs with a wide array of public and private higher education institutions. In 2016, AT&T sponsored a cybersecurity case study competition at Indiana University. Additionally, many K-12 schools participate in the Air Force Association's Cyber Patriot National Youth Cyber Education Program, of which AT&T is a Diamond Sponsor. Coaches across the country come from all sectors, including communications.
    d. A committee member works at Ivy Tech Community College as full-time assistant professor teaching Cyber Security and Information Assurance. He offers a view of how higher education institutions can help lead the way in training and education: Ivy Tech has been designated a National Center of Academic Excellence in Information Assurance 2-Year Education by the National Security Agency and the Department of Homeland Security. https://news.ivytech.edu/2012/05/21/ivy-tech-community-college-designated-center-of-academic-excellence-in-information-assurance/
    e. Ivy Tech has a cybersecurity student club on campus where students meet weekly and train for Cyber Security state, national, and international competitions such as:
        i. National Cyber League (NCL) https://www.nationalcyberleague.org/
        ii. US Cyber Challenge (USCC) http://www.uscyberchallenge.org/
        iii. Colligate Cyber Defense Competition (CCDC) http://www.cssia.org/ccdc/
        iv. National Security Agency (NSA) Codebreaker Challenge https://nationalccdc.org
    f. Ivy Tech also provides cybersecurity awareness for the community during the National Cyber Security Awareness Month sponsored by Department of Homeland Security and invited Cyber Security IT Professionals and Law Enforcement Agencies

Forensic Intelligence analyst to speak to our students, faculty, staff, and the public "about Cyber Security awareness."

g. Other organizations represented by committee members also volunteer to provide Cyber Security Awareness information across public events, typically in coordination with Cyber Security Awareness activities in October.

2. What (or who) are the most significant cyber vulnerabilities in your area?

a. For the communications sector in a general sense, vulnerabilities that have the potential to reduce or significantly impair service pose the greatest risk. Many communications services rely on the ability to transmit information in near real time. Any disruption to these services can have a vast impact on the public and to critical safety and private industry activities. As such, the class of threats generally known as Denials of Service or Distributed Denials of Service (DDoS) are extremely significant within the communications sector.

b. Also, vulnerabilities that could lead to information disclosure are significant and extremely important. Loss of customer information (CPNI), intellectual property, business plans, and information that could lead to a threat actor being able to compromise operational practices all fall into this category and are generally related to information technology (IT) infrastructure security.

c. Finally, a class of cybersecurity vulnerabilities that lead to fraudulent consumption of pay services tends to be important to the communications sector.

3. What is your area's greatest cybersecurity need and/or gap?

a. Sharing of threat information across public and private sector boundaries and within the broader sector continues to be of critical importance. Significant improvements have been made over the past fifteen years. However, there is still a lot of room for additional improvement.

b. Some hard and soft barriers to making effective use of information sharing in the communications sector are at play: For starters, the use of technology to enable rapid information sharing is available, but not close to universal adoption. The Structured Threat Information eXpression (STYX) and Trusted Automated eXchange of Indicator Information (TAXII) protocols for threat information sharing have helped by enabling technologies to communicate at machine speed. However, coordination and response still occurs largely at human speed, and often with significant organizational latency. Additional investment in and adoption of cyber response automation is needed across the sector.

c. The communications sector is also made up of a complex blend of regulatory and legally mandated responsibilities that do not easily keep up with the pace of cyber threats and exploits. A simplification of this landscape could help accelerate cyber response times.

d. Finally, organizational latency can likely be reduced by simplifying or reducing penalties associated with cybersecurity operational practice. In order for responses to proliferate through the sector at the speed of an attack, organizations must be made to feel empowered to take action without needing to evaluate the risk of penalty for acting or sharing on information that is not otherwise compulsory.

4. What federal, state, or local cyber regulations is your area beholden to currently?

a. The regulated portion of the communications sector is regulated at the State level by the Indiana Utilities Regulatory Commission and at the Federal level by the Federal Communications Commission. At the Federal level, the following are major pieces of legislation that govern the sector:

   i. The Communications Act of 1934

   ii. The Cable Communications Policy Act of 1984

iii. The Cable Television Consumer Protection and Competition Act of 1992
iv. The Telecommunications Act of 1996

b. Public policy implementation has been guided by and interpreted broadly by the FCC as well as in United States case law, such as *Comcast Corp. v. FCC (2010).*
c. Title 170 of the Indiana Administrative Code establishes the framework through which the IURC operates to develop and adopt rules and regulations concerning practice, procedure, and standards of service.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
   a. The United States Department of Homeland Security is home to many programs and bodies that deal with whole sector and whole nation cybersecurity planning, information sharing, and response activities. Indiana and sector members across the spectrum already participate in most of these programs.
   b. Key programs from which this Council can learn include but are not limited to: The DHS Sector-Specific Plans, MS-ISAC, NCC, NSTAC, and NCIRP. These are all mature programs intended to foster public/private partnerships across a range of activities, including cyber defense and planning.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, white papers, articles, books, etc. Please collect and document.**
   a. Article outlining the value of early cyber education in Israel: https://www.dailynews.com/2017/02/04/in-israel-teaching-kids-cyber-skills-is-a-national-mission/
   b. DHS 2015 Sector-specific Plan: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf
   c. US-CERT National Cyber Incident Response Plan: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
   d. Johns Hopkins Applied Physics Laboratory paper on a Cybersecurity framework known as Integrated Adaptive Cyber Defense (IACD): https://secwww.jhuapl.edu/IACD/Resources/OnePagers/Autoimmunity-for-CTI-Sharing-One-Pager-200.pdf
   e. BurningGlass.org Cybersecurity job market analysis: http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
   f. War on the Rocks article on the Cyber Security workforce gap as a National Security concern: https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/
   g. ISC2 Article on the growing Cyber Security workforce gap: http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
   a. Many Colleges and Universities in other states are starting to become a Center of Academic Excellence in cyber education. Here is the current list by the NSA/DHS:
      i. https://www.cybersecuritymastersdegree.org/dhs-and-nsa-cae-cd-designated-schools-by-state/
   b. Also, other states Colleges and Universities have on campus Cyber Security Club and Cyber Security Training Centers. To mention a few for example are DePaul University and Moraine Valley Community College.

i. DePaul University Cyber Club is a leader in Cyber Security Competition: https://www.depaulnewsline.com/debuzz/depaul-cyber-security-team-places-third-national-competition
ii. Moraine Valley Community College is a leader in Cyber Training: https://www.morainevalley.edu/news-story/hub-for-cybersecurity-training-at-moraine-valley/

8. What does success look like for your area in one year, three years, and five years?

a. One year success should be measured in terms of getting sector roles, responsibilities, and partnerships across public/private and intra-sector boundaries clarified and simplified as related to cyber planning and response. Heading into 2019, there should be significant momentum towards more effective partnering in real time operational actions bolstered by clear and tested operational planning.
b. Three-year measures of success should include a significant reduction in organizational latency in these partnerships, which should be achieved through technical, operational, and public policy improvements.
c. Across all sectors, we believe that a critical measure of success in five years is a significant closing of the cybersecurity skills gap in the workforce. This may present an economic development opportunity for Indiana, and it is crucial for the long-term viability of all industries.

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

a. Recommendations:
   - We do not know of any schools in Indiana that are a CAE Center of Academic Excellence in Cyber Operations. So Indiana has no CAE in CO yet. Please see the list below for the entire USA: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/centers.shtml
   - We do not know of any schools in Indiana that are a National Center for Systems Security and Information Assurance (CSSIA). This is critical for training Indiana faculty, Students, and the public in Cyber Education. For Example, Illinois has CSSIA at Moraine Valley Community College. http://www.cssia.org/
   - We believe that we need to provide early public cybersecurity education starting at K-12, please see this article. https://www.edweek.org/ew/articles/2017/03/22/with-hacking-in-headlines-k-12-cybersecurity-ed.html
     Also, we need to promote and involve many k-12 schools in cyber education training. https://www.k12cybersecurityconference.org/
     Furthermore, public schools should be encouraged to consider participating in the Air Force Association's Youth Cyber Education Program, called Cyber Patriot: https://www.uscyberpatriot.org/
   - We recommend that we must make it a mandatory part of our College Education in Indiana for students attending college to take a course in cybersecurity awareness. Please see this article about early cybersecurity education in Israel. https://www.dailynews.com/2017/02/04/in-israel-teaching-kids-cyber-skills-is-a-national-mission/

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

burningglass CAREERS IN FOCUS

Appendix 1: State Data

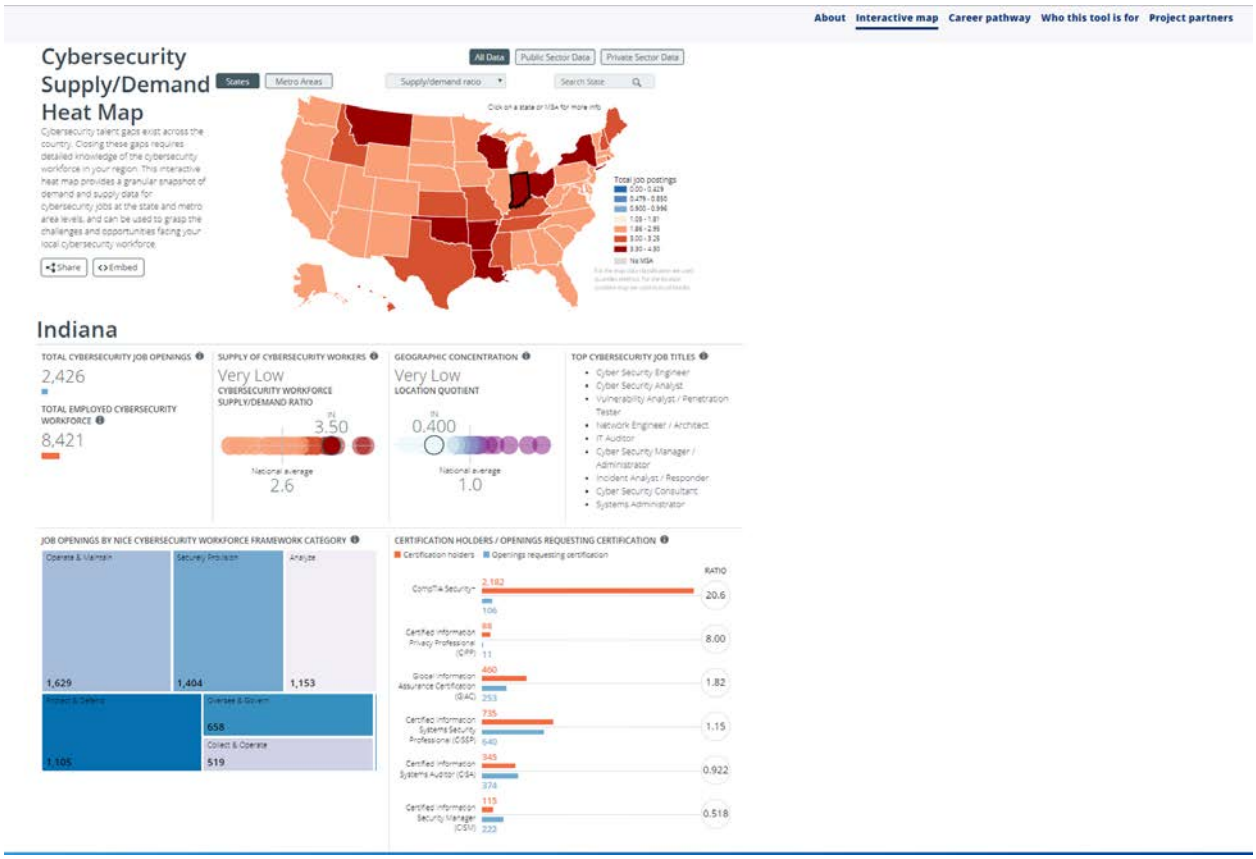
	State	Total Postings	Location Quotient*	% Growth (2010-2014)
1	Alabama	2,159	0.66	31%
2	Alaska	556	1.00	17%
3	Arizona	5,502	1.18	87%
4	Arkansas	989	0.5	117%
5	California	28,744	1.02	75%
6	Colorado	7,688	1.77	111%
7	Connecticut	2,771	0.97	98%
8	Delaware	1,152	1.67	92%
9	Florida	9,847	0.67	135%
10	Georgia	8,757	1.22	121%
11	Hawaii	1,364	1.31	39%
12	Idaho	634	0.53	260%
13	Illinois	11,428	1.16	163%
14	Indiana	2,347	0.48	139%
15	Iowa	1,951	0.74	158%
16	Kansas	1,654	0.71	168%
17	Kentucky	1,753	0.58	209%
18	Louisiana	1,563	0.48	275%
19	Maine	791	0.74	214%
20	Maryland	11,406	2.40	39%
21	Massachusetts	7,911	1.45	92%
22	Michigan	4,225	0.59	117%
23	Minnesota	4,059	0.88	98%
24	Mississippi	827	0.45	161%
25	Missouri	4,004	0.86	88%

	State	Total Postings	Location Quotient*	% Growth (2010-2014)
26	Montana	344	0.43	189%
27	Nebraska	1,603	1.00	68%
28	Nevada	1,462	0.70	89%
29	New Hampshire	581	0.50	134%
30	New Jersey	8,268	1.21	80%
31	New Mexico	1,003	0.72	119%
32	New York	14,089	0.97	104%
33	North Carolina	7,503	1.06	127%
34	North Dakota	322	0.49	341%
35	Ohio	6,281	0.72	141%
36	Oklahoma	1,476	0.53	196%
37	Oregon	2,618	0.89	136%
38	Pennsylvania	5,745	0.59	69%
39	Rhode Island	1,267	1.53	134%
40	South Carolina	2,312	0.69	134%
41	South Dakota	354	0.50	195%
42	Tennessee	2,340	0.51	97%
43	Texas	18,525	0.92	113%
44	Utah	1,371	0.61	146%
45	Vermont	281	0.52	168%
46	Virginia	20,276	3.09	38%
47	Washington	5,119	0.96	94%
48	West Virginia	496	0.41	35%
49	Wisconsin	2,429	0.51	139%
50	Wyoming	176	0.37	245%

*Location quotients show how concentrated demand is in a particular geography relative to employment in that area. National location quotient equals 1.0; an LQ of 1.2 indicates that demand is 20% more concentrated than nationally.

© 2015 Burning Glass Technologies 16

a. Since wide swaths of the communications sector operate both nationally and internationally, the workforce statistics specific to Indiana cybersecurity-related jobs presents a misleading picture of the sector's preparedness to plan for and respond to events. We've provided a more generalized assessment of the workforce challenges that appear to be universally impactful across sectors:
    i. By researching online and reading the report that is published by Burning glass at Job Market Intelligence Cyber Security Jobs as of 2015, we noted that there is a total posting of 2,347 cybersecurity jobs with Location Quotient of 0.48 and Growth Percentage of 139% between 2010 to 2014. http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
b. Also, according to the article "THE CYBER WORKFORCE GAP: A NATIONAL SECURITY LIABILITY?", which clearly indicates the widespread issue, Indiana's gap is wider than the US average.
    a. "Current data shows a talent shortfall of 40,000 unfilled cybersecurity jobs per year in the United States, with a growing international talent gap to match."
    b. https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/
c. The entire world also has a shortfall of workers "CYBERSECURITY WORKFORCE SHORTAGE PROJECTED AT 1.8 MILLION BY 2022" according to this website http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html
d. Finally, according to CyberSeek.org interactive map, it shows that the supply of cybersecurity workers in Indiana is at Very Low with cybersecurity workforce Supply/Demand Ratio at 3.5 (see image below):



<u>Indiana Data between October 2016 through September 2017</u>

e. TOTAL CYBERSECURITY JOB OPENINGS: 2,426
   a. Shows the number of online job listings for cybersecurity-related positions
f. TOTAL EMPLOYED CYBERSECURITY WORKFORCE: 8,421
   a. Shows the estimated number of workers employed in cybersecurity-related jobs in 2016. This includes workers in primary cybersecurity jobs – such as cybersecurity analysts – as well as workers in roles requiring cybersecurity-related skills and certifications to capture the full potential cybersecurity workforce.
g. Please see the above interactive map at: http://cyberseek.org/heatmap.html

11. What do we need to do to attract cyber companies to Indiana?

a. If all traditional economic factors are accounted for, the single biggest incentive to attracting cyber companies and jobs to Indiana will be to outpace other states and regions in the creation of a dynamic and highly educated cybersecurity workforce. If the workforce is supplemented with a rich ecosystem of organically generated start-up companies and public sector opportunities to attract external talent as well, this could represent a long-term growth opportunity for the State.
b. Execution of this growth would require targeted and sustained investment as well as an aggressive campaign to differentiate Indiana's opportunity in comparison to more traditional technology hubs.

12. What are your communication protocols in a cyber emergency?

a. The communications sector follows the communication protocols as defined by the Department of Homeland Security and the US-CERT National Cyber Incident Response Plan as documented below.

i. DHS 2015 Sector-specific Plan: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf
ii. US-CERT National Cyber Incident Response Plan: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

b. If a cyber event manifests as or is concurrent with a natural or man-made disaster impacting critical infrastructure, we would additionally follow guidelines associated with the Federal Emergency Management Agency's (FEMA) National Incident Management System (NIMS):
   i. FEMA NIMS FAQ: https://www.fema.gov/pdf/emergency/nims/nimsfaqs.pdf

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. Operationalize knowledge of FEMA's National Incident Management System (NIMS): https://www.fema.gov/pdf/emergency/nims/nimsfaqs.pdf
b. Operationalize the US-CERT National Cyber Incident Response Plan: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
c. Participate in sector-specific or multi-state Information Sharing Analysis Centers (ISAC): https://www.nationalisacs.org/member-isacs
d. Incorporate threat information sharing technologies, such as STYX/TAXII to move towards machine time as opposed to human time sharing of threat information.
e. Work towards more real-time response technologies and automation to significantly reduce organizational latency in the response to cyberattacks.
f. Invest in cybersecurity awareness training for employees, customers, and your local communities

Deliverable: Voluntary Industry Contact List

Deliverable: Voluntary Industry Contact List

General Information

1. **What is the deliverable?**
   a. Establish Voluntary Industry Contact List

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Both the State and other sectors will know who to contact in the associations, companies, and individuals within the Communications Sector, in the event of a cyber incident. Ultimately, the list will help facilitate communication with entities.

6. **What metric or measurement will be used to define success?**
   a. Participation % of companies and individuals to the list

7. **What year will the deliverable be completed?**
   a. While we hope to establish the list in 2018, it will be an ongoing item that will need to be maintained.

8. **Who or what entities will benefit from the deliverable?**
    a. The State and other cybersecurity stakeholders.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Unknown.

Additional Questions:

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana's Broadband Innovation Group
    b. Indiana Broadband and Technology Association
    c. Satellite Industry Association
    d. Indiana Exchange Carrier Association
    e. Other companies and organizations in the communications sector.

12. **Who should be main lead of this deliverable?**
    a. Joni Hart will work with other stakeholders to gather the appropriate information.

13. **What are the expected challenges to completing this deliverable?**
    a. TBD

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Research Contact Points/Structure	Joni Hart	95%	9-26-18	
Design Survey	Joni Hart	50%	9-26-18	
Review/Survey Appropriate Housing of Data Collected	Joni Hart	50%	9-26-18	
Provide Draft Survey to Sector Members	Joni Hart	25%	9-26-18	
Assign Members to assist with subsector response	Joni Hart	25%	9-1-18	

Assign Members to research other state data points	Joni Hart	25%	9-1-18	
Survey Response Deadline	Joni Hart	95%	9-14-18	
Prepare List for Committee Review	TBA	0%	10-1-18	
Finalize Deliverable	TBA	0%	10-29-18	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
CSP List	Outreach/ensure participation	$0	Minimal	-	-	-

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The contact lists will facilitate communication between the state and communications sector, and possibly other sectors working with the communications sector.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Ideally, facilitating communication and reducing time for contact collection during an incident can reduce time and expenses.

19. What is the risk or cost of not completing this deliverable?

a. Undeterminable

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Sector participation of 70%

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. TBD

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Hesitation for members to contribute data to the state, hesitancy to promote regulation, lack of response, and multi-state contacts for companies.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Administrative support in updating the list.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Limited

27. Can this deliverable be used by other sectors?

a. TBD-will need to assess if members view contacts to be public
b. **If Yes, please list sectors**

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. TBD-will need to assess if members view contacts to be public

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No

30. What are other public relations and/or marketing considerations to be noted?

a. None

Evaluation Methodology

Objective 1: Develop a form and process to collect a central cyber industry contact list by October 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Seventy percent of all communications providers complete annual cyber contact form by December 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Communications Sector Terminology Glossary

Deliverable: Communications Sector Terminology Glossary

General Information

1. **What is the deliverable?**
   a. Communications Sector Terminology Glossary

2. **What is the status of this deliverable?**
   a. Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. The glossary is intended to provide definition of terminology unique to the communications sector to reduce friction in cross-sector planning and response activities

6. **What metric or measurement will be used to define success?**
   a. Publication of peer-reviewed glossary that removes friction in cross-sector communications regarding cybersecurity incidents.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. All Indiana critical infrastructure sectors can benefit from a better understanding of the communications sector.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None identified

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Public Safety Committee

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Communications sector entities and industry groups will be consulted in the creation of this glossary.

12. **Who should be main lead of this deliverable?**
    a. Dan Solero

13. **What are the expected challenges to completing this deliverable?**
    a. The communications sector is complex. This complexity will present major challenges in completing a comprehensive and useful document.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Phase 1 questionnaire	Dan Solero	100	Feb, 2018	Complete
Phase 2 questionnaire	Dan Solero	100	Mar, 2018	Complete
Draft document outline	Dan Solero	100	July 1, 2018	Complete
Assign sections to committee members for authorship	Dan Solero	100	July 14, 2018	Complete
Review completed first draft document sections for content	Dan Solero	100	August 1, 2018	Complete
Revise document based on feedback and edit for flow and grammar	Dan Solero	100	August 9, 2018	Complete
Publish release 1 of paper to Syncplicity and IECC website	Dan Solero	100	September 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The greatest benefit to the glossary is in the reduction of friction related to understanding the complexities and jargon associated with the communications sector. A better understanding of the unique terminology of the communications sector will help with broad planning and execution in the face of chaos associated with a widespread cyberattack.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will not directly reduce risk, but may alleviate impact by facilitating faster, better coordinated, and more robust response from the communications sector

19. What is the risk or cost of not completing this deliverable?

a. Without this glossary, the communications sector will likely remain fairly opaque to processes and planning efforts in adjacent sectors.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion and publication of peer-reviewed glossary. (this is a binary metric. Completion and publication = success)

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Priorities related to committee member employers and personal commitments may impact timeline, as most members are volunteering their time and effort.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. This does not require sustained support.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Sector-specific associations and private sector companies.

27. Can this deliverable be used by other sectors?

a. Yes
   i. IT
   ii. Public Safety

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Industry associations, MS-ISAC, IN-ISAC, NCC, Comm-ISAC, National Cybersecurity and Communications Integration Center (NCCIC), privately held sector members.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. N/A

Evaluation Methodology

Objective 1: Complete Communications Sector Terminology Glossary by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Publish Communications Sector Terminology Glossary to IECC website by September 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☒ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Communications Sector Whitepaper

Deliverable: Communications Sector Whitepaper

General Information

1. **What is the deliverable?**
    a. Communications Sector Cyber Security Whitepaper

2. **What is the status of this deliverable?**
    a. In-progress; 50% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The whitepaper is intended to achieve several objectives, including:
        i. Definition of terminology unique to the communications sector to reduce friction in cross-sector planning and response activities
        ii. Description of typical roles, responsibilities, and incident response practices as well as governing regulations, frameworks, and laws that influence or guide communications sector entities in risk management, threat sharing, operational practice, and incident response
        iii. Mapping and inventory of national, regional, and local entities and services that make up the communications sector in Indiana

6. **What metric or measurement will be used to define success?**
    a. Publication of peer-reviewed whitepaper that facilitates deeper understanding of the communications sector and how its cybersecurity interests are managed and defined

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. All Indiana critical infrastructure sectors can benefit from a better understanding of the communications sector.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None identified

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Public Safety Committee

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Communications sector entities and industry groups will be consulted in creation of this paper.

12. **Who should be main lead of this deliverable?**
    a. Dan Solero

13. **What are the expected challenges to completing this deliverable?**
    a. The communications sector is complex. This complexity will present major challenges in completing a comprehensive and useful document.

Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Phase 1 questionnaire	Dan Solero	100	Feb, 2018	Complete
Phase 2 questionnaire	Dan Solero	100	Mar, 2018	Complete
Draft document outline	Dan Solero	100	July 1, 2018	Complete
Assign sections to committee members for authorship	Dan Solero	50	September 1, 2018	Sections will be reassigned for completion upon forming the next IECC.
Review completed first draft document sections for content	Dan Solero	0	September 29, 2018	May reschedule deadline earlier depending on schedules.
Submit reviewed draft document broadly to industry groups, subject matter experts, and peer sectors for comment.	Dan Solero	0	September 29, 2018	This will align to first draft deadline
Revise document based on feedback and edit for flow and grammar	Dan Solero	0	October 14, 2018	
Publish release 1 of white paper to Syncplicity and IECC web site	Dan Solero	0	October 29, 2018	Dependency on final draft revision schedule.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The greatest benefit to the whitepaper is in reduction of friction related to understanding the complexities and jargon associated with the communications sector. Better understanding of the unique characteristics of the communications sector will help with broad planning and execution in the face of chaos associated with a wide spread cyberattack.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will not directly reduce risk, but may alleviate impact by facilitating faster, better coordinated, and more robust response from the communications sector

19. What is the risk or cost of not completing this deliverable?

a. Without this whitepaper, the communications sector will likely remain fairly opaque to processes and planning efforts in adjacent sectors.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion and publication of peer and industry-reviewed whitepaper. (this is a binary metric. Completion and publication = success)
b. Adoption or adaptation of the paper by other jurisdictions or projects. If the paper is well received, other jurisdictions or projects will likely want to use it or adapt it to their use. Baseline is zero, since it does not yet exist. Any adoption or adaptation for use should be viewed as a measure of success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Priorities related to committee member employers and personal commitments may impact timeline, as most members are volunteering their time and effort.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. This does not require sustained support.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Sector-specific associations and private sector companies.

27. Can this deliverable be used by other sectors?

a. Yes
   i. IT
   ii. Public Safety

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Industry associations, MS-ISAC, IN-ISAC, NCC, Comm-ISAC, NCCIC, privately held sector members.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. N/A

Evaluation Methodology

Objective 1: Complete the Communications Sector Whitepaper for industry by October 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Distribute the Communications Sector Whitepaper to eighty percent of identified industry and key stakeholders by November 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☒ Focus Group
☒ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Cyber Incident Response Engagement Guide

Deliverable: Cyber Incident Response Engagement Guidance

General Information

1. **What is the deliverable?**
   a. Cyber Incident Response Engagement Guidance for Communications Sector

2. **What is the status of this deliverable?**
   a. In-progress; 25% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable:

5. **What is the resulting action or modified behavior of this deliverable?**
   a. The document intends to provide operational guidance on how communications sector principals should be engaged in the event of widespread cyberattack. The resulting action should be faster and more complete engagement of the communications sector in incident response engagements and planning.

6. **What metric or measurement will be used to define success?**
   a. Publication of peer-reviewed and industry-supported engagement guidance document.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. All Indiana critical infrastructure sectors can benefit from a better understanding of the communications sector.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None identified

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Public Safety Committee

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Communications sector entities and industry groups will be consulted in the creation of this paper.

12. **Who should be main lead of this deliverable?**
    a. Dan Solero

13. **What are the expected challenges to completing this deliverable?**
    a. The communications sector is complex. This complexity will present major challenges in completing comprehensive and useful guidance.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Phase 1 questionnaire	Dan Solero	100	Feb, 2018	Complete
Phase 2 questionnaire	Dan Solero	100	Mar, 2018	Complete
Research similar engagement guidance documents from adjacent sectors or similar projects	Dan Solero	0	September 1, 2018	Will be assigned at upcoming committee meeting
Draft document outline	Dan Solero	50	September 1, 2018	In progress
Assign sections to committee members for authorship	Dan Solero	0	September 14, 2018	Will be assigned at upcoming committee meeting
Review completed first draft document sections for content	Dan Solero	0	September 30, 2018	May reschedule deadline earlier depending on schedules.
Submit reviewed draft document broadly to industry groups, subject matter experts, and peer sectors for comment.	Dan Solero	0	October 14, 2018	This will align to first draft deadline
Revise document based on feedback and edit for flow and grammar	Dan Solero	0	October 29, 2018	
Publish release 1 of document to Syncplicity	Dan Solero	0	November 14, 2018	Aligned to final draft revision schedule.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The greatest benefit of the whitepaper will be to better facilitate advanced planning and cross-sector alignment around incident response.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will not directly reduce risk, but may alleviate impact by facilitating faster, better coordinated, and more robust response from the communications sector

19. What is the risk or cost of not completing this deliverable?

a. Without this document, response coordination may be complicated by needing to research and conduct outreach within the response window. Without the ability to plan ahead, robust response engagement will be extremely challenging.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion and publication of the industry-reviewed document. (this is a binary metric. Completion and publication = success)
b. Approval of the engagement guidance by sector members and industry associations will be an indicator of success.
c. Use of the document or adaptation by similar projects or working groups should also be viewed as a measure of success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Priorities related to committee member employers and personal commitments may impact timeline, as most members are volunteering their time and effort.
b. Some industry members may have governing regulations that complicate completion of this guidance on schedule.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. This does not require sustained support.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Sector-specific associations and private sector companies.

27. Can this deliverable be used by other sectors?

a. Yes
    i. IT
    ii. Public Safety

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Industry associations, MS-ISAC, IN-ISAC, NCC, Comm-ISAC, NCCIC, privately held sector members.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No
    i. The information included in this document may be deemed to disclose operational practices that members do not wish to make available to the public. If at all possible, we would like for the document to be available to the public. This decision will depend on feedback from sector members.

30. What are other public relations and/or marketing considerations to be noted?

a. N/A

Evaluation Methodology

Objective 1: Develop the Communications Sector Engagement Guidance by October 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Distribute the Communications Sector Engagement Guidance to eighty percent of identified industry and key stakeholders by December 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☒ Scorecard Comparison
☒ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Telecommunication Terms

IECC Communications Committee

Telecommunication Terms

August 2018

Telecommunication Terms

ACCESS CHARGE
A fee charged subscribers or other telephone companies by a local exchange carrier for the use of its local exchange networks.

ADSL
Asymmetric digital subscriber line (**ADSL**) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voiceband modem can provide. ADSL differs from the less common symmetric digital subscriber line (SDSL). In ADSL, bandwidth and bit rate are said to be asymmetric, meaning greater toward the customer premises (downstream) than the reverse (upstream). Providers usually market ADSL as a service for consumers for Internet access for primarily downloading content from the Internet, but not serving content accessed by others.

ANALOG SIGNAL
A signaling method that uses continuous changes in the amplitude or frequency of a radio transmission to convey information.

BANDWIDTH
The width of a communications channel. In analog communications, bandwidth is typically measured in Hertz. In digital communication, bandwidth is measured in bits per second (bps).

BROADBAND
In telecommunications, broadband means a wide range of frequencies over which information can be transmitted.
A simple way to compare broadband and narrowband Internet connections is to picture a highway. Only one car can travel at a time on a one-lane highway (narrowband). However, when a highway is six or eight lanes wide (broadband), more traffic can drive on the road at the same time.

Think back to when you had a dial-up Internet connection. Now think about the Internet today. You have 'always-on' data connections that enable you to access multiple media sources and a wide range of information at the same time. That's broadband.

CARRIER
A company that is authorized by regulatory agencies to operate a telecommunications system. Examples include AT&T, Alltell, and Verizon.

CDMA (Code Division Multiple Access)
CDMA is a channel access method used by different radio communication technologies- one way to understand CDMA is to think of a party where everyone is talking at the same time. Lots of confusion, right? CDMA assigns different codes to each group of users, so other groups hear just noise-- and tune out.

CENTRAL OFFICE (CO)
In almost every neighborhood there is a windowless building that houses the switching equipment that connects your telephone to your neighbor's telephone or routes your call to another central office for long distance calls. This building is called the central office. The central office has switching equipment that can switch calls locally or to long-distance carrier phone offices.

CIRCUIT-SWITCHED NETWORK
Circuit-switched is a type of network in which a physical path is obtained for and dedicated to a single connection between two end-points in the network for the duration of the connection. Ordinary voice phone service is circuit-switched. The telephone company reserves a specific physical path to the number you are calling for the duration of your call. During that time, no one else can use the physical lines involved.

CLEC - Competitive Local Exchange Carrier
The Telecommunications Act of 1996 opened the door to competition for local phone service. This act mandated that the Incumbent Local Exchange Carriers (ILEC) such as Verizon, Bell South, or SBC provide the necessary interfaces so that CLECs could provide seamless local service. For example, MegaPath is a CLEC.

COMMON CARRIER
In the telecommunications arena, the term used to describe a telephone company.

COMMUNICATIONS ASSISTANT
A person who facilitates telephone conversation between text telephone users, users of sign language or individuals with speech disabilities through a Telecommunications Relay Service (TRS). This service allows a person with hearing or speech disabilities to communicate with anyone else via telephone at no additional cost.

COMMUNITY ANTENNA TELEVISION (CATV)
A service through which subscribers pay to have local television stations and additional programs brought into their homes from an antenna via a coaxial cable.

CPE (Customer Provided Equipment)
Telephone equipment (key systems, PBXs, answering machines, etc.) which live on the customer's premises.

CSP (Communication Service Provider)
An umbrella term used to describe both traditional providers of communication services (ie: telecom) and alternate providers such as cable TV companies and other over-the-top providers.

CSR - Customer Service Record
A copy of how your telephone records appear in your local carriers' database. It contains information items and charges such as: type of service, federal access charge, number portability charge, calling blocks on the line, 911 charge, etc. It is the "snapshot" of your entire service for each line.

DAC (Digital Analog Converter)
A device which converts digital pulses (ie: data) into analog signals so that the signal can be used by analog devices such as phones.

DC POWER PLANT
Each Central Office houses an AC power plant as well as an AC/DC converter that runs the majority of the telecommunications equipment. Some Central Office Technicians focus on keeping these power plants running efficiently 24/7.

DIAL AROUND
Long distance services that require consumers to dial a long-distance provider's access code (or "10-10" number) before dialing a long-distance number to bypass or "dial around" the consumer's chosen long-distance carrier in order to get a better rate.

DIGITAL TELEVISION (DTV)
A new technology for transmitting and receiving broadcast television signals. DTV provides clearer resolution and improved sound quality.

DIRECT BROADCAST SATELLITE (DBS/DISH)
A high-powered satellite that transmits or retransmits signals which are intended for direct reception by the public. The signal is transmitted to a small earth station or dish (usually the size of an 18-inch pizza pan) mounted on homes or other buildings.

DSL (Digital Subscriber Line)
The technology used between a customer's premises and the telephone company to support the transport of higher bandwidth digital signals on the copper twisted wire pairs already in place as part of the telephony infrastructure. Also known as generic name signifying the family of Digital Subscriber Line technologies including ADSL, HDSL, VDSL, etc.

DSLAM
A DSLAM (Digital Subscriber Line Access Multiplexer) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line (DSL) connections and puts the signals on a high-speed backbone line using multiplexing techniques. Depending on the product, DSLAM multiplexers connect DSL lines with some combination of asynchronous transfer mode (ATM), frame relay, or Internet Protocol networks. DSLAM enables a phone company to offer business or homes users the fastest phone line technology (DSL) with the fastest backbone network technology (ATM).

DSO, DS1 & DS3 (Digital Signal 0, 1, 3, etc)
Different levels of digital hierarchy for the amount and speed of data carried on a circuit. The fundamental speed level is DS-0, which is a voice grade channel.

DWDM (Dense Wave Division Multiplexing)
The higher-capacity version of WDM, which is a means of increasing the capacity of fiber-optic data transmission systems through sending many wavelengths of light down a single strand of fiber.

ENHANCED SERVICE PROVIDERS
A for-profit business that offers to transmit voice and data messages and simultaneously adds value to the messages it transmits. Examples include telephone answering services, alarm/security companies and transaction processing companies.

EnodB
E-UTRAN Node B, also known as Evolved Node B (abbreviated as eNodeB or eNB), is the element in E-UTRA of LTE that is the evolution of the element Node B in UTRA of UMTS. It is the hardware that is connected to the mobile phone network that communicates directly wirelessly with mobile handsets (UEs), like a base transceiver station (BTS) in GSM networks.

Traditionally, a Node B has minimum functionality, and is controlled by a Radio Network Controller (RNC). However, with an eNB, there is no separate controller element. This simplifies the architecture and allows lower response times.

FTTC, FTTH, FTTB
Think "Fiber to the ____". In the acronyms above, the ____ is Cabinet, Home and Business and relate to optical fiber extensions. Translation? Access networks that consist of optical fiber from the exchange to the cabinet//home/business.

FACILITY (facilities)
A facilities person assigns the cable or fiber pair numbers. The facilities assignment refers to where the telephone number starts in the central office and the route it takes from the central office to the end address (includes those boxes you see on the side of the street).

FEMTOCELLS
Femtocells enhance coverage and capacity inside buildings which means fewer dropped calls. This has potential to allow cell phone calls to travel over the internet. *"Femtocells. They will be everyplace. And the cheaper they are, the easier to install. the better coverage you get."* - Ivan Seidenberg, CEO Verizon

FIBER / FIBER OPTIC CABLE
Transmits light signals along glass strands, permitting 10-100 times faster transmission than traditional copper wire. What this means to the consumer, is faster, more efficient cell phones and Internet connections.
You may hear FTTH (fiber to the home), FTTP (fiber to the premises). Those terms simply mean – how close the fiber comes to a building, house…end user. The closer it comes, the faster the connection.

FRAME
A rack to which telecommunications equipment is mounted. You will see these in Central Offices.

FRAME RELAY
The standard for high-speed data communications, offering users transmission speeds of 2.048 megabits per second and higher. It allows faster speeds than the X.25 packet switching standard because it does away with elaborate error-correction and routing information. Its main application is interconnecting local area networks.

FREQUENCY MODULATION (FM)
A signaling method that varies the carrier frequency in proportion to the amplitude of the modulating signal.

GLOBAL POSITIONING SYSTEM (GPS)
A US satellite system that lets those on the ground, on the water or in the air determine their position with extreme accuracy using GPS receivers.

HCS (Hierarchical Cell Structure)
Hierarchical Cell Structure: the architecture of a multi-layered cellular network where subscribers are handed over from the macro to the micro to the pico layer, depending on the current network capacity and the needs of the subscriber.

HD VOICE
A technology that provides better audio quality by delivering at least twice the sound range (wideband) of a traditional (narrowband) telephone call.

HDSL (High Bit Rate Digital Subscriber Line)
This is digital access technology typically used by businesses. It requires two copper wire pairs (or in some cases fiber) but doesn't require complex engineering and installation.

HSPA (High Speed Packet Access)
Often referred to as 3.5G, this is an extension to the original 3G standard providing significantly higher data rates. HSDPA (downlink) can provide theoretical maximum downlink speeds of 168 Mbps. HSUPA (uplink) supports maximum uplink speeds of 22 Mbps.

INFRASTRUCTURE
This is an incredibly important part of the communications industry. Roughly 25% of all telecom workers are involved with telecom infrastructure – in its simplest terms, infrastructure includes the pieces and parts that make sophisticated communications systems work.

INTERACTIVE VIDEO DATA SERVICE (IVDS)
A communication system, operating over a short distance, that allows nearly instantaneous two-way responses by using a hand-held device at a fixed location. Viewer participation in game shows, distance learning and e-mail on computer networks are examples.

INSTRUCTIONAL TELEVISION FIXED SERVICE (ITFS)
A service provided by one or more fixed microwave stations operated by an educational organization and used to transmit instructional information to fixed locations.

IPTV (Internet Protocol Television)
Digital television delivered over the Internet. It can be accessed through a closed or public network, with a computer or a set-top box capable of processing the video streams. This is in direct competition with traditional cable and broadcast television. IPTV can be bundled with VoIP and Internet access for a triple play service, increasing the competition that other television providers face.

ISDN
Integrated Services Digital Network (**ISDN**) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. The ISDN standards define several kinds of access interfaces, such as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).

ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s.

L2TP (Layer 2 Tunneling Protocol)
Layer 2 Tunneling Protocol is an IETF (Internet Engineering Task Force) standard tunneling protocol for VPNs. ISPs use this to provide secure, node to node communications in support of multiple, simultaneous tunnels in the core of the internet or IP based networks.

LANDLINE
Traditional wired phone service.

LAND MOBILE SERVICE
A public or private radio service providing two-way communication, paging and radio signaling on land.

LATA - Local Access and Transport Area
Geographic area covered by one or more local telephone companies, which are legally referred to as local exchange carriers (LECs). A connection between two local exchanges within the LATA is referred to as intraLATA. A connection between a carrier in one LATA to a carrier in another LATA is referred to as interLATA. InterLATA is long-distance service. The current rules for permitting a company to provide intraLATA or interLATA service (or both) are based on the Telecommunications Act of 1996.

LOW POWER FM RADIO (LPFM)
A broadcast service that permits the licensing of 50-100 watt FM radio stations within a service radius of up to 3.5 miles and 1-10 watt FM radio stations within a service radius of 1 to 2 miles.

LOW POWER TELEVISION (LPTV)
A broadcast service that permits program origination, subscription service or both via low powered television translators. LPTV service includes the existing translator service and operates on a secondary basis to regular television stations. Transmitter output is limited to 1,000 watts for normal VHF stations and 100 watts when a VHF operation is on an allocated channel.

LTE (Long Term Evolution)
LTE is a broadband access technology that enhances the ability of mobile users to access larger amounts of data. LTE operates on a lower frequency of 700 MHz giving it enhanced signal range and building/obstacle penetration. AT&T and Verizon Wireless are building their 4G networks with LTE technology.

This is a big deal because for the most part, consumers want more and more data. In fact, a recent IBM report shows that when people are asked what they would be least likely to cut back on to save money - people chose mobile phones and broadband Internet only after their homes.

MICROCELL
A **microcell** is a cell in a mobile phone network served by a low power cellular base station (tower), covering a limited area such as a mall, a hotel, or a transportation hub. A microcell is usually larger than a picocell, though the distinction is not always clear. A microcell uses power control to limit the radius of its coverage area.

Typically, the range of a microcell is less than two kilometers wide, whereas standard base stations may have ranges of up to 35 kilometers (22 mi). A picocell, on the other hand, is 200 meters or less, and a femtocell is on the order of 10 meters, although AT&T calls its femtocell that has a range of 40 feet (12 m), a "microcell".

MICROWAVE
A common form of transmitting telephone and data conversations that occupies a very high frequency range and produces a signal good for about 30 miles.

MMS (Multimedia Messaging Service)
The standard in mobile messaging services, adding photos, pictures and audio to text messages.

MOBILE BROADBAND
Wireless high-speed internet access through a portable modem, telephone or other device.

MUST-CARRY (Retransmission)
A 1992 Cable Act term requiring a cable system to carry signals of both commercial and noncommercial television broadcast stations that are "local" to the area served by the cable system.

MUX - MULITPLEX
To transmit two or more signals over a single channel. In the world of CAT5 the explosion of choices that digital TV is bringing the multiplex means to offer subscribers a choice of various starting times for movies and events.

NETWORK
A telecommunications network is a collection of terminals, links and nodes which connect together to enable telecommunication between users of the terminals. Networks may use circuit switching or message switching. Each terminal in a network must have a unique address so messages or connections can be routed to the correct one.
*Wikipedia definition

NETWORK OPERATIONS CENTER (NOC)
A **network operations center** (or **NOC**, pronounced "knock") is one or more locations from which control is exercised over a computer, television broadcast or telecommunications network.

NUMBER PORTABILITY
A term used to describe the capability of individuals, businesses and organizations to retain their existing telephone number(s) — and the same quality of service — when switching to a new local service provider.

OPEN VIDEO SYSTEMS
An alternative method to provide cable-like video service to subscribers.

OPERATOR SERVICE PROVIDER (OSP)
A common carrier that provides services from public phones, including payphones and those in hotels/motels.

OUTSIDE PLANT
Refers to all of the physical cabling and supporting infrastructure (such as conduit, cabinets, tower or poles), and any associated hardware (such as repeaters) located between a demarcation point in a switching facility to another switching facility or to a customer premises.

PACKET SWITCHING
Packet switching is a method of grouping data which is transmitted over a digital network into *packets* which are made of a header and a payload. Data in the header is used by networking hardware to direct the packet to its destination where the payload is extracted and used by application software. Packet switching is the primary basis for data communications in computer networks worldwide.

PAGING SYSTEM
A one-way mobile radio service where a user carries a small, lightweight miniature radio receiver capable of responding to coded signals. These devices, called "pagers," emit an audible signal, vibrate or do both when activated by an incoming message.

PBX
Private Branch Exchange Digital or analog telephone switchboard located on the customer premises and used to connect private and public telephone networks.

PBX (Private Branch Exchange)
A private (as in owned by the telephone company) exchange (as in the Central Office). A PBX is a small version of the phone company's larger central switching office. In other words, an analog telephone switchboard located on the customer premises and used to connect private and public telephone networks.

PERSONAL COMMUNICATIONS SERVICE (PCS)
Any of several types of wireless, voice and/or data communications systems, typically incorporating digital technology. PCS licenses are most often used to provide services similar to advanced cellular mobile or paging services. However, PCS can also be used to provide other wireless communications services, including services that allow people to place and receive communications while away from their home or office, as well as wireless communications to homes, office buildings and other fixed locations.

PLANT
A general term for all equipment used by a telephone company to provide telecommunications services. In the telecom business, plant comes in two variations – inside and outside plant. Inside is in a building. Outside is outside the building – on poles, in the ground.

POTS
Plain old telephone service (POTS), or plain ordinary telephone service, is a retronym for voice-grade telephone service employing analog signal transmission over copper loops. POTS was the standard service offering from telephone companies from 1876 until 1988 when the Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) was introduced, followed by cellular telephone systems, and voice over IP (VoIP). POTS remain the basic form of residential and small business service connection to the telephone network in many parts of the world. The term reflects the technology that has been available since the introduction of the public telephone system in the late 19th century, in a form mostly unchanged despite the introduction of Touch-Tone dialing, electronic telephone exchanges and fiber-optic communication into the public switched telephone network (PSTN).

PRESCRIBED INTEREXCHANGE CHARGE (PICC)
The charge the local exchange company assesses the long-distance company when a consumer picks it as his or her long-distance carrier.

PSTN
The public switched telephone network (PSTN) is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephone operators, providing infrastructure and services for public telecommunication. The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers, thus allowing most telephones to communicate with each other. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core network and includes mobile and other networks, as well as fixed telephones.

RAN
A **radio access network** (**RAN**) is part of a mobile telecommunication system. It implements a radio access technology. Conceptually, it resides between a device such as a mobile phone, a computer, or any remotely controlled machine and provides connection with its core network (CN). Depending on the standard, mobile phones and other wireless connected devices are varyingly known as user equipment (UE), terminal equipment, mobile station (MS), etc. RAN functionality is typically provided by a silicon chip residing in both the core network as well as the user equipment.

RBOC (Regional Bell Operating Company)
There are seven (also known as Baby Bells) which own the local exchange carriers in the US following the divestiture/breakup of AT&T ('Ma Bell') in 1984.

ROAMING
The use of a wireless phone outside of the "home" service area defined by a service provider. Higher per-minute rates are usually charged for calls made or received while roaming. Long distance rates and a daily access fee may also apply.

SS7
Signaling System No. 7 (SS7) is a set of telephony signaling protocols developed in 1975, which is used to set up and tear down most of the world's public switched telephone network (PSTN) telephone calls. It also performs number translation, local number portability, prepaid billing, Short Message Service (SMS), and other mass market services.

In North America it is often referred to as *CCSS7*, abbreviated for *Common Channel Signaling System 7*. In the United Kingdom, it is called *C7* (CCITT number 7), *number 7* and *CCIS7* (Common Channel Interoffice Signaling 7). In Germany, it is often called ZZK-7 (*Zentraler ZeichengabeKanal Nummer 7*).

SATELLITE
A radio relay station that orbits the earth. A complete satellite communications system also includes earth stations that communicate with each other via the satellite. The satellite receives a signal transmitted by an originating earth station and retransmits that signal to the destination earth station(s). Satellites are used to transmit telephone, television and data signals originated by common carriers, broadcasters and distributors of cable TV program material.

SATELLITE UPLINK
Uplink refers to a transmission of data in which data flows from a ground-based transmitter to an orbital satellite receiver. Uplink is used to send data to a satellite in Earth’s orbit in order to make changes to the way the satellite functions or simply redirect data to another ground-based receiver. Uplink is used in every application that involves the use of an orbital satellite and is a necessary component of all satellite-based telecommunications systems. Like downlink, uplink depends on the use of C Band, Ku Band, and Ka Band radio frequencies, although the frequency ranges differ in downlink and uplink applications.

SERVICE PLAN
The rate plan you select when choosing a wireless phone service. A service plan typically consists of a monthly base rate for access to the system and a fixed amount of minutes per month.

SERVICE PROVIDER
A telecommunications provider that owns circuit switching equipment.

SPLICE
The joining of two or more cables together by splicing the conductors together. In copper wire telephone cables, splicing is on a mechanical basis and pair-to-pair, with the pairs organized by binder groups and color codes. In optical fiber cables, the splicing is fiber-to-fiber, with the fibers organized by ribbon or colored buffer tube and color code. Fiber optics splicing may be either mechanical splicing or fusion splicing.

SUBSCRIBER LINE CHARGE (SLC)
A monthly fee paid by telephone subscribers that is used to compensate the local telephone company for part of the cost of installation and maintenance of the telephone wire, poles and other facilities that link your home to the telephone network. These wires, poles and other facilities are referred to as the "local loop." The SLC is one component of access charges.

SWITCH - SWITCHING
A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. In the traditional circuit-switched telephone network, one or more switches are used to set up a dedicated though temporary connection or circuit for an exchange between two or more parties. On an Ethernet local area network (LAN) a switch determines from the physical device (Media Access Control or MAC) address in each incoming message frame which output port to forward it to and out of. In a wide area packet-switched network such as the Internet, a switch determines from the IP Address in each packet which output port to use for the next part of its trip to the intended destination. * definition from whatis.com

TARIFF
The documents filed by a carrier describing their services and the payments to be charged for such services.

TELECOMMUNICATIONS
Transmitting signals over a distance in order to communicate. The classic 'tin can' telephone is a very simple telecommunications system. Emerging technologies have brought us far from that model. Today's communication could be via telephone, television, radio, satellite, wireless network, computer network, telemetry, or other means. These technologies, plus many more are converging—you can access the Internet, play videos, or track your children's movements via global positioning system (GPS) technology on your cell phone—so the lines between telecommunications and other industries like computer hardware, application software, consumer electronics and entertainment are getting blurrier all the time.

TELECOMMUNICATIONS CIRCUIT
A telecommunication circuit is any line, conductor, or other conduit by which information is transmitted. Originally, this was analog, and was often used by radio stations as a studio/transmitter link (STL) or remote pickup unit (RPU) for their audio, sometimes as a backup to other means. Later lines were digital and used for private corporate data networks.

TELECOMMUNICATIONS RELAY SERVICE (TRS)
A free service that enables persons with TTYs, individuals who use sign language and people who have speech disabilities to use telephone services by having a third party transmit and translate the call.

TELECOMMUNICATIONS SYSTEMS
Networks of leading-edge technologies such as fiber optic systems, satellites, wireless, telephony, and cable, which are connected to computers that allow organizations and individuals throughout business and industry to communicate instantaneously around the world.

TELEPHONE EXCHANGE
A telephone exchange is a telecommunications system used in the public switched telephone network or in large enterprises. An exchange consists of electronic components and in older systems also human operators that interconnect (*switch*) telephone subscriber lines or virtual circuits of digital systems to establish telephone calls between subscribers.

TELEPHONE LINE
A telephone line or telephone circuit (or just line or circuit within the industry) is a single-user circuit on a telephone communication system. This is the physical wire or other signaling medium connecting the user's telephone apparatus to the telecommunications network, and usually also implies a single telephone number for billing purposes reserved for that user. Telephone lines are used to deliver landline telephone service and Digital subscriber line (DSL) phone cable service to the premises. Telephone overhead lines are connected to the public switched telephone network.

TELEPHONE NUMBER
A telephone number is a sequence of digits assigned to a fixed-line telephone subscriber station connected to a telephone line or to a wireless electronic telephony device, such as a radio telephone or a mobile telephone, or to other devices for data transmission via the public switched telephone network (PSTN) or other private networks.

TELEPHONY
The word used to describe the science of transmitting voice over a telecommunications network.

TIRKS (Trunks Integrated Record Keeping System)
An operations support system developed by the Bell System during the late 1970s. It was developed for inventory and order control management of interoffice trunk circuits that interconnect telephone switches. It grew to encompass and automate many functions required to build the ever-expanding data transport network. Supporting circuits from POTS and 150 baud modems up through T1, DS3, SONET and DWDM, it continues to evolve today, and unlike many software technologies today, provides complete backward compatibility. TIRKS is in use at AT&T, Verizon, CenturyLink, and Cincinnati Bell Telephone.

TOLL
A device that receives calls and allows them to be transmitted to the next local calling area, thus avoiding toll or access charges.

TRUNK / TRUNKING
A communication line between two switching systems. The term switching system typically includes equipment in a Central Office and PBXs. A tie trunk connects PBXs. Central office trunks connect a PBX to the switching system at the Central Office.

TTY
A type of machine that allows people with hearing or speech disabilities to communicate over the phone using a keyboard and a viewing screen. It is sometimes called a TDD.

TWISTED CABLE PAIR
Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of improving electromagnetic compatibility. Compared to a single conductor or an untwisted balanced pair, a twisted pair reduces electromagnetic radiation, crosstalk between neighboring pairs and improves rejection of external electromagnetic interference. It was invented by Alexander Graham Bell.

UNIVERSAL SERVICE
The financial mechanism which helps compensate telephone companies or other communications entities for providing access to telecommunications services at reasonable and affordable rates throughout the country, including rural, insular and high costs areas, and to public institutions. Companies, not consumers, are required by law to contribute to this fund. The law does not prohibit companies from passing this charge on to customers.

VDSL
Very-high-bit-rate digital subscriber line (VDSL) and very-high-bit-rate digital subscriber line 2 (VDSL2) are digital subscriber line (DSL) technologies providing data transmission faster than asymmetric digital subscriber line (ADSL).

VDSL offers speeds of up to 52 Mbit/s downstream and 16 Mbit/s upstream, over a single flat untwisted or twisted pair of copper wires using the frequency band from 25 kHz to 12 MHz. These rates mean that VDSL is capable of supporting applications such as high-definition television, as well as telephone services (voice over IP) and general Internet access, over a single connection. VDSL is deployed over existing wiring used for analog telephone service and lower-speed DSL connections

VIDEO HEADEND
The Video Headend is the point in the network which linear (e.g., broadcast TV) and on-demand (e.g., movies) content is captured and formatted for distribution over a network. The headend ingests national feeds of linear programming via satellite either directly from the broadcaster or programmer or via an aggregator. The Headend takes each individual channel and allows the operator the option to use RF or encode it into digital video format, like Mpeg 2 or Mpeg 4, for both standard (SD) and high definition (HD) television signals. This digital video formatted content is then ingested into a Quam or IP network for delivery.

VIVID
The acronym VIVID includes each component of the evolving communications industry: Voice, Information, Video, Infrastructure & Data. Check out our Industry Overview page to see some of the vivid components of telecom in action.

VOICE
Audible communication over a traditional land-line, wireless cellular or smart phone or even through a computer via VOIP.

VOIP (Voice over Internet Protocol)
Harnesses the power of broadband internet connections to allow consumers access to telephone services over the internet. In other words, your words get converted into data signals and travel over the internet. Once they get to their destination, they are converted from data signals back into analog signals and transmitted. Upgrades in technology helped combat problems with early VoIP, such as poor quality and availability of service. Today's VoIP is a viable competitor to traditional telephony. As businesses continue to cut costs and limit travel budgets, expect to see the use of VoIP increase.

VoLTE
VoLTE, or Voice Over LTE is similar to VoIP- but goes one step further. Instead of using the hardware at the ends of the call (the phones), VoLTE offloads the heavy lifting to the network- creating VoIP HD. Beyond a crisp and clear sound, VoLTE includes the ability to cancel echos and background noise on the back end, not the handset itself *.
*definition taken from pocketnow.com

WIDE AREA NETWORK (WAN)
A computer or communications network that covers a geographic area which is larger than a business campus. Usually, the dividing line between a local or campus network and an Wide Area Network is a router. On the local or campus side, the transmission lines in a network (copper or fiber) are usually owned by the enterprise. On the WAN side, the lines are typically owned by a carrier and leased to an enterprise.
By far, the most familiar – and largest WAN is the Internet.

WIRELESS
Wireless telecommunications carriers provide telephone, Internet, data, and other services to customers through the transmission of signals over networks of radio towers. The signals are transmitted through an antenna directly to customers, who use devices, such as cell phones and mobile computers, to receive, interpret, and send information.

3G and 4G
These terms refer to third- and fourth-generation cellular wireless capabilities. 3G and 4G networks allow mobile and smart phone users to access more information and services on their devices faster. It's because of these technological advances that you can video chat, watch Internet TV, play online games, download videos and listen to streaming music on your phone. Simply put, 3G and 4G allow you to do more.

Both 3G and 4G—now enhanced by LTE technology—are available across most of the U.S. today. The major difference between the two is speed. In general, 4G LTE networks are much faster than 3G LTE networks.

5G

Fifth-generation wireless, or 5G, is the latest iteration of cellular technology, engineered to greatly increase the speed and responsiveness of wireless networks. With 5G, data transmitted over wireless broadband connections could travel at rates as high as 20 Gbps by some estimates -- exceeding wireline network speeds -- as well as offer latency of 1 ms or lower for uses that require real-time feedback. 5G will also enable a sharp increase in the amount of data transmitted over wireless systems due to more available bandwidth and advanced antenna technology.

APPENDIX D.2
DEFENSE INDUSTRY COMMITTEE

DEFENSE INDUSTRY COMMITTEE STRATEGIC PLAN

Chair: Danielle Chrysler | Co-Chair: Kyle Werner

September 2018
Indiana Executive Council on Cybersecurity

Defense Industry Committee Plan

Contents

Committee Members **4**
Introduction **6**
Executive Summary **8**
Research **14**
Deliverable: Cyber Market System **18**
General Information 18
Implementation Plan 19
Evaluation Methodology 23
Deliverable: Cyber Digital Platform **25**
General Information 25
Implementation Plan 27
Evaluation Methodology 32
Deliverable: Cyber Statewide Testbed **34**
General Information 34
Implementation Plan 35
Evaluation Methodology 39
Supporting Documentation **41**

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Danielle Chrysler	IODD	Executive Director	Chair	Voting
Kyle Werner	Crane	Strategic Director	Co-Chair	Advisory
Kurt Huff	Raytheon	Director	Full Time	Contributing
Andrew Baker	Rolls Royce	Director	Full Time	Contributing
Sandeep Allam	St. logics	Owner	Full Time	Contributing
Ryan Metzing	Ice Miller (Began work under Aerospace & Defense Council)	Director	Full Time	Advisory
JJ Thompson	Rook Security	Owner	Full Time	Advisory
Tony Vespa	Vespa Group	Owner	Full Time	Advisory
Dave Roberts	IEDC	Director	Full Time	Voting Proxy
General Cliff Tooley	NCCO	Director	Full Time	Advisory
Colonel Pfaff	Indiana Guard	Director	As Needed	Contributing
Dr. Templeman	Crane	Director	As Needed	Contributing

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - The Defense Industry Committee leveraged a recently completed Indiana Office of Defense Development (IODD)/Sagamore Institute study of Indiana's defense market, insights provided by state small and large cybersecurity business leaders, a review of the State's current cybersecurity-related web presence, and defense cybersecurity-related academic programs to establish a baseline for how the defense industry might contribute to the effort to enhance the cybersecurity posture of the State of Indiana and its critical assets.
    - Sagamore / IODD detailed Defense Report (current standings in Defense programs)
    - Other State's Cybersecurity Defense Industry
    - Other State's Current Programs supporting Defense Industry
    - Current Asset Inventories of programs, partnerships and current contract proposals
    - Sensitive Compartmented Information Facility (SCIF) Inventory
    - Current cybersecurity industry numbers

- **Research Findings**
  - Our analysis of the defense cybersecurity industry landscape in Indiana led to three conclusions:
    - The defense cybersecurity industry ecosystem within the state provides the Governor with a potentially potent weapon in his kitbag to promote the State as a leader in cybersecurity locally, regionally and nationally.
    - Indiana's defense industry has a strong desire to support the Governor's effort to enhance the cybersecurity posture of the State and its critical assets.
    - As it is at the national level, the foundation of Indiana's cybersecurity is a strong state economy supported by 21st Century public policy that provides the environment, resources and impetus to reposition Indiana as a thought and action leader in the cybersecurity space nationally and internationally.
  - These conclusions led the committee to establish preliminary declarations of its group ethos and mission that reads as follows:
    - The foundation of Indiana's security is a strong economy. In the 21st Century, that economy is defined by a digital world wherein cyber threats pose a clear and present danger. The first protection principle for Indiana's security is the existence of a robust defense cybersecurity industry whose presence and participation serves as a natural inoculation against threats emerging from the cyber vector.
    - Therefore, the mission of the Defense Committee is to seek, encourage and promote programs and projects that lead to the growth of a vibrant cybersecurity defense industry-related economy within the State of Indiana.

- **Additional Findings**
  - The committee's initial research established the following as preliminary facts related to the State's cybersecurity defense industry:
    - The state's private sector cybersecurity defense industry is limited when compared to other states claiming leadership nationally with only thirteen companies identified as being current players in this market segment. However, those companies are extremely motivated to play a larger role at the state, regional and national levels, but require the support of the state in doing so.
    - The state's federal sector cybersecurity footprint represents great potential for leveraging via public-private partnerships in advancing Indiana's interests with the inventory including Naval Surface Warfare Center Crane, the Indiana National Guard's Muscatatuck training and testing facility, the Indiana National Guard's Stout Field Special Compartmented Information Facility (SCIF) and cybersecurity support team, and Grissom Air Reserve Base's cyber team.
    - Under the leadership of the Lieutenant Governor, the state has taken the initial first steps towards repositioning Indiana in the defense cybersecurity market through the commissioning of a statewide defense industry study directed towards framing a way ahead for the state in establishing itself as a thought and action leader in this market and has initiated the implementation of that study's principle recommendations which include:
      - The establishment of a statewide defense market development and capture system.
      - The establishment of a statewide strategy for repositioning Indiana as a defense market thought and action leader.
      - The establishment and operation of a public-private partnership digital and physical defense industry ecosystem with the cybersecurity market being its first major vector.

- **Committee Deliverables**
  - Cyber Market System
  - Cyber Digital Platform
  - Cyber Statewide Testbed

- **Additional Notes / Way Ahead:**
  - The Defense Industry Committee has identified the following two tasks as being those that frame the way ahead:
    - Working closely with the Lieutenant Governor in integrating its efforts with those directed towards the larger state-level defense market development and capture system.
    - Identifying and advocating public-private partnership opportunities to advance the development and growth of the defense cybersecurity market within the State.

- **References**

  - Accenture, *Integrated Digital Platforms: Flexible Technology to Meet the Consumer* Challenge, (Accenture Interactive: 2012)
  - AcqNotes, *Acquisition Process*, http://acqnotes.com/acqnote/acquisitions/acquisitionprocess-overview

- AcqNotes, *Acquisition Category (ACAT),* http://acqnotes.com/acqnote/acquisitions/acquisition-category
- Aerospace Industries Association, *The Strength to Lift America: The State of the U.S. Aerospace and Defense Industry,* (AIA: 2016)
- American Legislative Exchange Council, *Rich States, Poor States – ALEC-Laffer State Economic Competitiveness Index*, (ALEC: 2017)
- APMP Center for Business Development Excellence, *Capability Maturity Model for Business Development, Version 2.0* (APMP: 2014)
- Arellano, Robert, *Analysis of Rapid Acquisition Processes to Fulfill Future Urgent Needs*, (Naval Postgraduate School: 2015)
- BD-CMM Development Team and Steering Committee, *Capability Maturity Model for Business Development, Version 1.0*, (Business Development Institute: 2007)
- Center for Strategic and International Studies, *Defense Acquisition Trends, 2016 – The End of the Contracting Drawdown*, (CSIS: 2017)
- Centers for Disease Control and Prevention, *Contracting Process,* https://www.cdc.gov/contracts/process/index.html
- Congressional Research Service, *Defense Primer: The National Defense Budget Function (050),* (CRS: 2017)
- CNBC, *America's Top States for Business 2017*, https://www.cnbc.com/2017/07/11/americas-top-states-for-business-2017-overallranking.html
- DB4 Consulting, *Capture Management: Art, Science or Sorcery?* (Loudon County Chamber of Commerce GovCon Initiative Training Session: 2015)
- Defense Acquisition University, *Defense Acquisition Guidebook*, https://www.dau.mil/tools/dag
- Defense Science Board, *Fulfillment of Urgent Operational Needs*, (USD AT&L: 2009) Defense Systems Management College, *DoD Funds Management Platinum Card,* (Defense Acquisition University, Fort Belvoir, VA: 2016).
- Deloitte, *2017 Global Aerospace and Defense Sector Outlook – Growth Prospects Remain Upbeat*, (Deloitte: 2017)
- Deputy Assistant Secretary of Defense, Emerging Capability and Prototyping (EC&P), *Prototyping and Experimentation: Accelerating the Adoption of Transformative Capabilities*, (DASD EC&P: 2016)
- DeVol, Ross, Joe Lee and Minoli Ratnatunga, *2016 State Technology and Science Index,* (Milken Institute: 2016) 37
- Douglas, Brad, *Welcome to the New Normal: Winning Business in Today's Market Place*, (Deltek Insight 2015: 2015)
- Etherton, Jon, *Acquisition Policy: Current Acquisition Environment*, (NDIA: 2017)
- Evans, Peter, Annabelle Gawer, *The Rise of the Platform Enterprise: A Global Survey*, (The Center for Global Enterprise: 2016)
- Federal Procurement Data System-Next Generation, *Top 100 Contractors Report Fiscal Year 2016*, (GSA, https://www.fpds.gov/fpdsng_cms/index.php/en/reports/62-top-100-contractors-report)
- Gates, Doug, Tom Mayor, Erich Gampenrieder, *Global Aerospace and Defense Outlook: The Dawn of a New Day*, (KPMG: 2016)
- Goodly, Bernard, *Managing the Army's Research and Development Investments in a Time of Declining Resources*, (Defense Acquisition University: 2016)
- Governing for States and Localities, *Military Active-Duty Personnel, Civilians by State*, http://www.governing.com/gov-data/military-civilian-active-duty-employee-workforcenumbers-by-state.html

- Government Accountability Office, *Contracting Data Analysis – Assessment of Government-wide Trends*, (GAO: 2017)
- Government Accountability Office, *Defense Science and Technology- Adopting Best Practices Can Improve Innovation Investments and Management*, (GAO: 2017)
- Government Accountability Office, *DoD Rapid Innovation Program – Some Technologies Have Transitioned to Military Users, but Steps Can Be Taken to Improve Program Metrics and Outcomes,* (GAO: 2016)
- GovernmentContractsWon.com, *Indiana Defense Contractor Lists by City*, https://www.governmentcontractswon.com/department/defense/indiana_cities.asp
- GovWin, *Top 20 Unrestricted Federal Business Opportunities for FY2018*, (Deltek Federal Information Solutions: 2017)
- Hahn, Heather, Maeve Gearing, Michael Katz, Ria Amin, *Observations of Leaders Driving Changes in State Government,* (Urban Institute: 2015)
- Indiana University *I-Light Network Map*, http://ilight.net/map
- Industrial Research Institute, *2017 Global R&D Funding Forecast*, (R&D Magazine: 2017)
- LeHong, Hung, Chris Howard, Dennis Gaughan, Debra Logan, *Building a Digital Business Technology Platform,* (Gartner: 2016)
- Levinson, Robert, Sopen Shah, Paige Connor, *Impact of Defense Spending: A State-by-State Analysis,* (Bloomberg Government: 2011)
- Linsscott, Warren, *2015 Deltek Clarity GovCon Industry Study Results*, (Deltek: 2015)
- Martin, Greg, *Lunch & Learn: Congressional Enactment*, (DAU: 2017)
- Milken Institute, *2016 State Technology and Science Index – Sustaining America's Innovation Economy*, (Milken Institute: 2016)
- Morgan, Steve. Cybersecurity Market Report, Q1 2017. http://cybersecurityventures.com/cybersecurity-market-report/
- Morgan, Steve. Cybersecurity Market Report, Q1 2017. http://cybersecurityventures.com/cybersecurity-market-report/
- Newman, Larry, *Shipley Proposal Guide for Business Development and Sales Professionals,* (Shipley Associates: 2009)
- Office of the Assistant Secretary of Defense for Research and Engineering, *DoD Laboratories and Centers*, https://www.acq.osd.mil/rd/laboratories/
- Office of the Secretary of Defense (Acquisition, Technology and Logistics), *Department of Defense Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) List*, (DoD: 2016) http://www.acq.osd.mil/ara/documents/mdap_mais_program_list_dated_01Nov16.pdf
- Office of the Secretary of Defense Test Resource Management Center, Test & Evaluation/Science & Technology Opportunities, June 8, 2015, http://slideplayer.com/slide/6052297/
- Office of the Undersecretary of Defense (Comptroller)/Chief Financial Officer, *Program Acquisition Cost by Weapon System United States Department of Defense*, (DoD: 2017)
- PricewaterhouseCoopers, *Aerospace and Defense 2016 in Review and 2017 Forecast*, (PwC: 2017)
- PricewaterhouseCoopers, *Aerospace Manufacturing Attractiveness Rankings*, (PwC: 2017)
- Project Management Institute, *PMBOK Guide, 6th Edition*, (Project Management Institute: 2017)
- Purdy, Ellen and Ted Bujewski, *Rapid Innovation Fund (RIF) 101*, (OSD Research and Engineering: 2017)

- Ross, Alec, "Want Job Security? Try online security". Wired, April 25, 2016
- Salesforce, *Federal Government Contractor Study 2016*, (Market Connections: 2016)
- Salesforce, *Government Contractor Best Practices*, (Market Connections, 2016).
- Sego, Patricia, *Capture Management*, (Glendale Technical Sales Consulting, Inc.: 2012)
- Shipley and Associates, *Business Development Lifecycle*, http://sbdl.shipleywins.com
- Shipley and Associates, *Business Development Lifecycle,* http://advancedpm.es/wpcontent/uploads/2015/04/Shipley-Business-Development-Process.jpg
- U.S. Department of Defense, *Department of Defense Directive 5000.01 Operation of the Defense Acquisition System*, (DoD: 2017)
- U.S. Department of Defense, *Department of Defense Instruction 5000.74, Defense Acquisition of Services*, (DoD: 2017)
- U.S. Department of Defense, *Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS),* (DoD: 2015)
- U.S. Department of Defense, *Performance of the Defense Acquisition System – 2016 Annual Report,* (DoD: 2016)
- U.S. Department of Defense, *Rapid Innovation Fund (RIF) Program: Use of Technology Transition Best Practices,* (DoD: 2016)
- U.S. Department of Defense, *Report to Congress- Restructuring the Department of Defense Acquisition, Technology and Logistics Organization and Chief Management Officer Organization*, (DoD: 2017)
- U.S. Department of Defense Office of Economic Adjustment, *Defense Spending by State Fiscal Year 2014*, (DoD OEA: 2016)
- U.S. Department of Defense Office of Economic Adjustment, *Defense Spending by State Fiscal Year 2015*, (DoD OEA: 2017)
- U.S. Department of Defense Office of Small Business Programs, *2017 Small Business Training Week – Rapid Innovation Fund*, (DoD OSBP: 2017)
- U.S. Department of Defense Rapid Reaction Technology Office, *Rapid Reaction Technology Office Overview*, (DoD RRTO: 2016)
- U.S. Department of Defense, *2016 Report to Congress: Sustainable Ranges*, (USD P&R: 2016)
- USASpending.gov, *Indiana Spending Map*, https://www.usaspending.gov/transparency/Pages/SpendingMap.aspx?statecode=IN
- Warley, David, *The Project Manager's Survival Guide to Bids, Tenders and Proposals*, (Association for Project Management: 2016)
- Whaley, Eileen and Dana Stewart*, Path from Urgent Operational Need to Program of Record*, (Defense Acquisition University Alumni Association: 2014)
- Wyatt, Earl, *Rapid Fielding: A Path for Emerging Concept and Capability Prototyping*, (DASD RF: 2013)

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Continued Defense Federal Acquisition Regulation (DFARS) training / software
    b. User training / programs to catch vulnerabilities

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. The everyday user
    b. Information Sharing Channels

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Studies have indicated that 60% of small business fail within 6 months of a significant cyber incident such as a breach or ransomware – Need affordable solutions to comply with current regulations and solution sets for the above statistics
    b. Technology Expertise
    c. Education and Training

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. DFARS compliance
    b. European Union's General Data Protection Regulation (GDPR)
    c. National Institute of Standards and Technology (NIST)

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Kentucky completed a full evaluation of Cyber in the State through Defense Office of Economic Adjustment (OEA) grant
    b. Cyber document – Indiana Economic Development Corporation (IEDC) 2017
    c. State of Illinois Cybersecurity Strategy

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. Defense Industry State Document – Sagamore Institute Produced
    b. Other State Research

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Private, Public, Partnership Investment in cybersecurity
    b. Innovation / Entrepreneur programs (California model)
    c. Defining the lane they want to dominate (Marketing plan and strategic plan attached)
    d. MiC3: Serving Michigan. The Michigan Cyber Civilian Corps (MiC3) is a group of trained cybersecurity experts who volunteer to provide expert assistance to enhance the State's ability to rapidly resolve cyber incidents when activated under a Governor declared State of Emergency. The group includes volunteers from government, education, and business sectors.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Cyber Defense Capture Market system by 2019
    b. Working Digital platform by 2019
    c. Industry Lead Cyber Conference 2019

d. Defense Industry Legislative Recommendations Summer 2019
e. 2% Market Share gain by 2022

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

a. Need to define exactly what you want to be in cyber, can't be the expert of all.

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. Indiana Based Cyber Focus companies
   i. Cimtrak (software)
   ii. Pondurance (services)
   iii. Rook Security (software and services)
   iv. RADcube (consulting and implementation)
   v. Gravicom, LLC
b. Cyber Focused companies with office in Indiana
   i. Optiv (reseller and services)
   ii. Proofpoint (software)
   iii. Mako Group
   iv. Rofori
c. Companies that do cyber but not as primary focus:
   i. EY
   ii. PwC
   iii. KSM
   iv. Crowe
   v. Raytheon
   vi. Vespa Group
d. Major Primes – All will have cyber experts inside protecting assets
e. Cybersecurity workforce – Needs to be defined and studied at a higher level

11. What do we need to do to attract cyber companies to Indiana?

a. Develop a market capture system that can truly identify opportunity in this sector
b. Land a large program of record / Department of Defense (DOD) Contract with cyber component (US Govt 19B in 2017)
c. Define focus in cyber
d. Invest money into the current assets (Georgia, Michigan, Rhode Island model)
e. Full inventory of all current assets (Kentucky model with OEA grant)
f. Consider models of Maryland's Cybersecurity Investment Incentive Tax Credit
g. Host conference or workshop on cyber insurance, funding risk assessments for critical infrastructure assets, piloting new technologies for critical infrastructure protection; and investing in processes to help critical infrastructure operators mitigate cyber risk. (already been offered by STLogics company in Indiana to host)

12. What are your communication protocols in a cyber emergency?

a. Internal Company protocols – Individually defined by each company

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. Partner with Industry. State governments can leverage partnerships with the private sector by utilizing industry expertise through the acquisition of products and services with high levels of security and reasonable terms and conditions.

b. Adopt Industry-Recognized Security Standards. State governments should adopt international standards recognized by industry to better align security across all agencies and departments.
c. Standardize Cloud Security. If state governments plan on standardizing their approach to cloud security, they should leverage existing federal certification programs at the state level.
d. Establish an Outcome Focused Governance Structure. A state's governance structure should cover all aspects of the enterprise and encourage cross-organizational collaboration and transparency.
e. Actively Share Information. There are a wide variety of different models for the sharing of cyber threat information, and integration centers have emerged in recent years to provide a vital link between all levels of government, the private sector, and academia.
f. Create a Culture of Awareness. State governments should invest in training and education for their workforces to enhance overall cybersecurity awareness

Deliverable: Cyber Market Systems

Deliverable: Cyber Market System

General Information

1. **What is the deliverable?**
    a. Indiana defense industry cybersecurity market pursuit collaboration plan and system.
    b. Define programs that are worthy of a collective Statewide program and complete asset mapping for what capabilities we have in the State.

2. **What is the status of this deliverable?**
    a. In-progress 80%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context**

    ☐ Establish an effective governing structure and strategic direction.
    ☒ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Reposition Indiana as a thought and action leader nationally and internationally in the defense cybersecurity market space. This platform will enable us to pull statewide and regional resources to compete in the national cyber market.

6. **What metric or measurement will be used to define success?**
    a. Two percent, about $300 million of DOD cybersecurity market share, around $15 billion plus, by Fiscal Year (FY) 2022 as identified in contracts and grants awarded captured in usaspending.gov

7. **What year will the deliverable be completed?**
    a. 2018
    b. Formalized Group 2018 – Defense Industry Cyber Committee
    c. Fully operationalized 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Indiana entrepreneurs, businesses, colleges, universities and agencies involved in the defense cybersecurity market space

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State and federal defense cybersecurity-related programs.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Economic Development
    b. Policy

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Economic Development Corporation, Crane, Indiana National Guard, National Center for Complex Operations, Inc., Sagamore Institute, Prime / Mid / Small Cybersecurity Industry, Indiana Office of Technology & Other State Resources.

12. **Who should be main lead of this deliverable?**
    a. Indiana Office of Defense Development (Danielle Chrysler) & Indiana Economic Development Corporation (Dave Roberts)

13. **What are the expected challenges to completing this deliverable?**
    a. None at this time

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Build Cyber Defense Team	IODD / IEDC	100%	January 1, 2018	Defense Industry Cyber Group will be Cyber lead for State Defense Effort with IEDC
Asset Mapping	IODD / IEDC	50%	January 1, 2019	Digital Platform will help us complete this process
Research National Cyber Opportunities	Defense Industry Committee / IEDC	50%	Ongoing	Working on group proposals for current opportunities
National & International Cybersecurity Market Development & Capture Support	IODD/IEDC/ NCCO	20%	Ongoing	Viable pursuit of opportunities requires sustained development & capture support.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No
   i. We will use current staff of IOT, IEDC, IODD and other entities to complete this process.

b. **If Yes, please complete the following:**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Digital Platform - Pilot	Establishes Base Line Cybersecurity Market Development & Capture Capability	$800K	N/A	OEA Grant	N/A	
Digital Platform – Phase 2	Digital Platform Marketing Capability	$10K	$10K / month	State	N/A	
Defense Cybersecurity Market Development & Capture Support	Viable market development & capture system requires persistent research & market analysis	$35K	$35K / month	State	N/A	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Provides state with capability to develop and capture national and international cybersecurity market share.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Indiana collectively has the resources to lead the national security dialogue in the cybersecurity space. No estimated cost at this time.

19. What is the risk or cost of not completing this deliverable?

a. Indiana currently has lost 60% of the market share in the DOD contracting space and the risk is to continue this losing trend when we have all the resources / companies to do business in the cybersecurity and DOD space.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Two percent increase in the Defense Market by 2022 / National recognition of Cyber capabilities in Indiana.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. State of Georgia – $40M to new cybersecurity building / assets – leaning in on future cyber solutions.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. See chart under question number 16.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Sagamore Institute – Outside think tank

27. Can this deliverable be used by other sectors?

a. Yes

b. **If Yes, please list sectors**

i. Cybersecurity marketing can be leveraged for adjacent markets and opportunities.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Indiana Office of Defense Development – Danielle Chrysler; Indiana Office of Economic Development (Defense Sector) – Danielle Chrysler (Innovation) – Dave Roberts

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes, but will require more discussion

30. What are other public relations and/or marketing considerations to be noted?

a. None

Evaluation Methodology

Objective 1: Indiana Office of Defense Development (IODD) and partners will develop and implement a cybersecurity market pursuit plan and system by January 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Digital Platform

Deliverable: Cyber Digital Platform

General Information

1. **What is the deliverable?**
    a. Indiana defense cybersecurity market development and capture plan and system (Digital Platform)

2. **What is the status of this deliverable?**
    a. Phase 1 - Pilot Phase 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☒ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Reposition Indiana as a thought and action leader nationally and internationally in the defense cybersecurity market space. This platform will enable us to pull statewide and regional resources to compete in the national cyber market.

i. This platform will allow Indiana business and academia to qualify and register as defense contractors. Once qualified and registered, the software platform will facilitate a streamlined and automated proposal and contract process, matching Government acquisition opportunities (e.g., Request for Information (RFI), Request for Proposal (RFP), Small Business Innovative Research and Small Business Technology Transfer (SBIR/STTR), and grants) to Indiana defense contractors.
ii. This platform will also allow Government and business users to perform Market Research, collect defense contract-related metrics, serve as a historical document, and "lessons-learned" repository and to allow post-contract award debriefs.

6. **What metric or measurement will be used to define success?**
    a. Two percent, about $300 million of DOD cybersecurity market share, around $15 billion plus, by Fiscal Year (FY) 2022 as identified in contracts and grants awarded captured in usaspending.gov.
    b. Percentage increase in defense spending executed through the digital platform.

7. What year will the deliverable be completed?
    a. 2018
    b. Pilot July 1, 2018
    c. Fully operationalized if funded by 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Indiana entrepreneurs, businesses, colleges, universities and agencies involved in the defense cybersecurity market space.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State and federal defense cybersecurity-related programs.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Economic Development
    b. Policy

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Economic Development Corporation, Crane, Indiana National Guard, National Center for Complex Operations, Inc., Sagamore Institute, Prime / Mid / Small Cybersecurity Industry, PTAC, Westgate/ARI, Indiana Universities, Atterbury-Muscatatuck.

12. Who should be main lead of this deliverable?

a. Indiana Office of Defense Development through the Office of Economic Adjustment Grant

13. What are the expected challenges to completing this deliverable?

a. State budget programmed funding for maintenance / upkeep of the platform

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Minimum Viable Product Phase 1	NCCO	100%	Jul 31, 2018	This is a pilot.
Marketing Plan	NCCO	0%	Aug 31, 2018	Unfunded
Training	NCCO	0%	Sep 31, 2018	Unfunded
Support	NCCO	0%	Jul 31, 2018	Unfunded
Scalable KCC Platform Phase 2	NCCO	0%	TBD	Unfunded

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
2 hours / week	1 hour / week	Product Sponsor (Business)	Office of Economic Adjustment (OEA) Grant	x	Product Owner-Decision Maker for product
2 hours / week	1 hour / week	Product Owner (Business)	OEA grant	x	Product Owner-Decision Maker for product
2 hours / week	1 hour / week	Product Technical Subject Matter Expert (Business)	OEA grant	x	Need at least one representative able to serve as a technical representative
2 hours / week	1 hour / week	Product Process Subject Matter Expert (Business)	OEA grant	x	Need one representative for each process owner if process has multiple owners

25 hours / week	25 hours / week	Product Build – Account Manager	OEA grant	x	
80 hours / week	80 hours / week	Business Analyst (Project Lead)	OEA grant	x	
40 hours / week	40 hours / week	Project Manager	OEA grant	x	
80 hours / week	80 hours / week	Front-End Developers	OEA grant	x	Need two or more
40 hours / week	40 hours / week	Lead System Architect	OEA grant	x	
80 hours / week	80 hours / week	Back-End Developers	OEA grant	x	Need two or more
0 hours / week	80 hours / week	Support Personnel (Business)	OEA grant	x	
0 hours / week	80 hours / week	Support Personnel (Technical)	OEA grant	x	
30 hours / week	30 hours / week	Training Personnel (Business)	OEA grant	x	Need three trainers
30 hours / week	30 hours / week	Training Personnel (Business)	OEA grant	x	Need three trainers

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Subscription Access to External and Government Databases	Data from External and Government Databases are required in order to supply the new product with needed information assets	$5,000	$500/month	OEA grant	x	Access to all databases
Cloud Infrastructure	This is required to host the application. Web Servers and Database Servers will be required.	$200,000	$15,000/month			

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. To increase the share of defense contracts in Indiana and ensuring that all the work is performed by companies, organizations and research institutions based in Indiana – analytics attached to the digital platform.
b. The major focus and benefit is job creation, more economic and business growth opportunities in Indiana and beyond.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Cybersecurity is the primary service category that the platform will capture and would enable organizations, academia and research institutions to provide risk reduction at the overall State level by developing capabilities and attracting and retaining talent.
b. Minimum viable product (MVP) cost is around $500 thousand and while the final costs are still being finalized it is generally in the range of 6-10 times the cost of MVP.

19. What is the risk or cost of not completing this deliverable?

a. Continue losing market share in the overall defense expenditure in State of Indiana.
b. Continue losing market share in the overall cybersecurity-related defense projects expenditure.
c. The limited capability of the tool will limit the amount of potential jobs created; as well as a limiting the contribution to economic prosperity and business potential in the State of Indiana.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Increased dollars from DoD funded contracts awarded to Indiana vendors.
b. Number of cybersecurity and defense contracts executed through the platform in automated fashion and in alignment with Defense Federal Acquisition Regulation (DFAR).
c. Increased number of Indiana jobs created by DoD funded contracts.
d. Baselines to be provided by DoD.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No
b. **If Yes, please list states/jurisdictions**
   i. N/A
   ii. From what we understand, the product being generated is the first of its kind for states / jurisdictions. The product will only generate more jobs, economic prosperity and business potential regardless of the current economic status of a given state/jurisdiction.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability and accessibility of key stakeholders / resources for critical information and support.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Strategic Guidance
b. Financial Support
c. Business Support
d. Technical Support

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. National Center for Complex Operations (NCCO)

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. Deliverable has unlimited use potential and can be used by any other federal agency

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Potential companies and users of the system.
b. IEDC, Indiana Procurement Technical Assistance Center (PTAC)
c. Academia and Research Institutions
d. NCCO and IODD internal users
e. Investors, Entrepreneurs, Donors

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes
    i. A safe, secure platform for connecting, vetting, and qualifying local vendors, national vendors, and government agencies.

30. What are other public relations and/or marketing considerations to be noted?

a. The site will be available via the web to the public and will be advertised on other websites / social media channels.

Evaluation Methodology

Objective 1: Indiana Office of Defense Development and partners will develop a pilot of the Indiana defense cybersecurity market development and capture plan and system (Digital Platform) by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indiana increases to two percent (about $300M) of the Department of Defense (DOD) cybersecurity market share ($15B plus) by FY 2022.
Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Cyber Statewide Testbed

Deliverable: Cyber Statewide Testbed

General Information

1. **What is the deliverable?**
    a. Indiana defense cybersecurity product test, training and demonstration plan and capability. (Cyber Statewide Testbed)

2. What is the status of this deliverable?
    a. In-progress 50%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Reposition Indiana as a thought and action leader nationally and internationally in the defense cybersecurity market space. This testbed will allow for companies, universities, local entities and military assets to test, train and demonstrate cyber capabilities.

6. **What metric or measurement will be used to define success?**
    a. Two percent, about $300 million of DOD cybersecurity market share, around $15 billion plus, by Fiscal Year (FY) 2022 as identified in contracts and grants awarded captured in usaspending.gov.

7. **What year will the deliverable be completed?**
    a. 2020
    b. Fully operationalized 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Indiana entrepreneurs, businesses, colleges, universities and agencies involved in the defense cybersecurity market space.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State and federal defense cybersecurity related programs.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Economic Development
    b. Policy

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Economic Development Corporation, Crane, Indiana National Guard, National Center for Complex Operations, Inc., Sagamore Institute, Prime / Mid / Small Cybersecurity Industry.

12. **Who should be main lead of this deliverable?**
    a. Indiana Office of Defense Development & Indiana Economic Development Corporation with technical expertise of Primes, Crane and Indiana National Guard assets and Indiana Office of Technology

13. **What are the expected challenges to completing this deliverable?**
    a. State budget programmed funding – (Georgia has put $40M towards Cybersecurity)

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Multi-Threat Energy Grid (M-TEG)	IEDC/NCCO	10%	January 2020	
Muscatatuck Cybertropolis (MUTC-C)	Indiana Guard	10%	January 2020	
Indiana Cyber Ecosystem (ICE)	IEDC/NCCO	0%	January 2020	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
5	5	Project Management	DOE Grant	X	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/ Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
M-TEG Design/Construct	Self-Explanatory	$22M	$1M / year	DOE Grant	X	
M-TEG Technical Project Lead & Analysis	Self-Explanatory	$1.2M	$1.2M / year	DOE Grant	X	
M-TEG Construction Project Manager & Required Studies	Self-Explanatory	$2.2M	$200K / year	DOE Grant	X	
M-TEG Program Management & Business Operations	Self-Explanatory	$1M	$1M / year	DOE Grant	X	
M-TEG Contingency	Self-Explanatory	$3.2M	N/A	DOE Grant	X	
M-TEG Phase II	Self-Explanatory	$20M	$20M	Private/State (80%/20%)	X	
M-TEG Phase III	Self-Explanatory	$20M	$20M	Private/State (80%/20%)	X	
Cybertropolis Project Management & Required Studies	Self-Explanatory	$1.5M	$1.5M	State	X	
Cybertropolis Design/Construct	Self-Explanatory	$10M	$10M	Private/State (80%/20%)	X	
Indiana Cyber Ecosystem	Self-Explanatory	$2M	$2M	State	X	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. This deliverable establishes Indiana as a thought and action leader in the national and international cybersecurity market.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable provides to the state, nation and world a capability to rapidly identify and respond to cyber threats against critical infrastructure.

19. What is the risk or cost of not completing this deliverable?

a. Indiana surrenders cybersecurity market dominance to other states.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success equals capture of five percent of international cybersecurity market share by end of calendar year 2023.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that do not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Award of DoE M-TEG Phase I grant.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. This deliverable will be self-sustaining through public-private business model no later than (NLT) end of calendar year 2022.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. IODD, NCCO, IEDC, state and national stakeholders.

27. Can this deliverable be used by other sectors?

a. Yes.

b. **If Yes, please list sectors**

i. Any sector involved in critical infrastructure and product protection training or testing will benefit from this deliverable.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Indiana Office of Defense Development and Indiana Economic Development Corporation.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. This deliverable will have an embedded public relations and marketing component.

Evaluation Methodology

Objective 1: Establish a nationally recognized cybersecurity test bed in Indiana by January 2020.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indiana captures five percent of international cybersecurity market share of cybersecurity test, training, and demonstration plan and capability by December 2023.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

No Supporting Documentation Provided At This Time

APPENDIX D.3
ECONOMIC DEVELOPMENT COMMITTEE

ECONOMIC DEVELOPMENT COMMITTEE STRATEGIC PLAN

Chair: Secretary Jim Schellinger | Co-Chair: Ron Pelletier

September 2018
Indiana Executive Council on Cybersecurity

Economic Development Committee Plan

Contents

Committee Members **4**

Introduction **6**

Executive Summary **8**

Research **12**

Deliverable: Incentive Program **17**

General Information 17

Implementation Plan 19

Evaluation Methodology 24

Deliverable: Implementation Plan for Cybersecurity - Marketing **26**

General Information 26

Implementation Plan 28

Evaluation Methodology 31

Deliverable: Cybersecurity SIoT Innovation District **33**

General Information 33

Implementation Plan 35

Evaluation Methodology 38

Supporting Documentation 40

Indiana Economic Development Corporation Cyber Initiative Report 41

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Positon	IECC Membership Type
Jim Schellinger	Indiana Economic Development Corporation	Secretary	Chair	Voting
Ron Pelletier	Pondurance	Founding Partner	Co-Chair	Voting
David Roberts	Indiana Economic Development Corporation	Chief Innovation Officer	Chair Proxy	Voting Proxy
Dennis Porter	Pondurance	Director of Operations & Administration	Co-Chair Proxy	Advisory
Jason Ortiz	Pondurance	Senior Software Engineer	Full Time	Advisory
Mark Wasky	Indiana Economic Development Corporation	VP & Counsel, Government & Community Affairs	Full Time	Advisory
Jamie Lee	Wabash National Corporation	CIO, VP of IT	Full Time	Advisory
Teresa Lubbers	Indiana Commission for Higher Education	Commissioner	Full Time	Voting
Doug Rapp	Cyber Leadership Alliance	President	Full Time	Advisory
Leon Ravenna	KAR Auction Services	CISO	Full Time	Advisory
Geanie Umberger	Purdue University	Associate Dean for Engagement	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

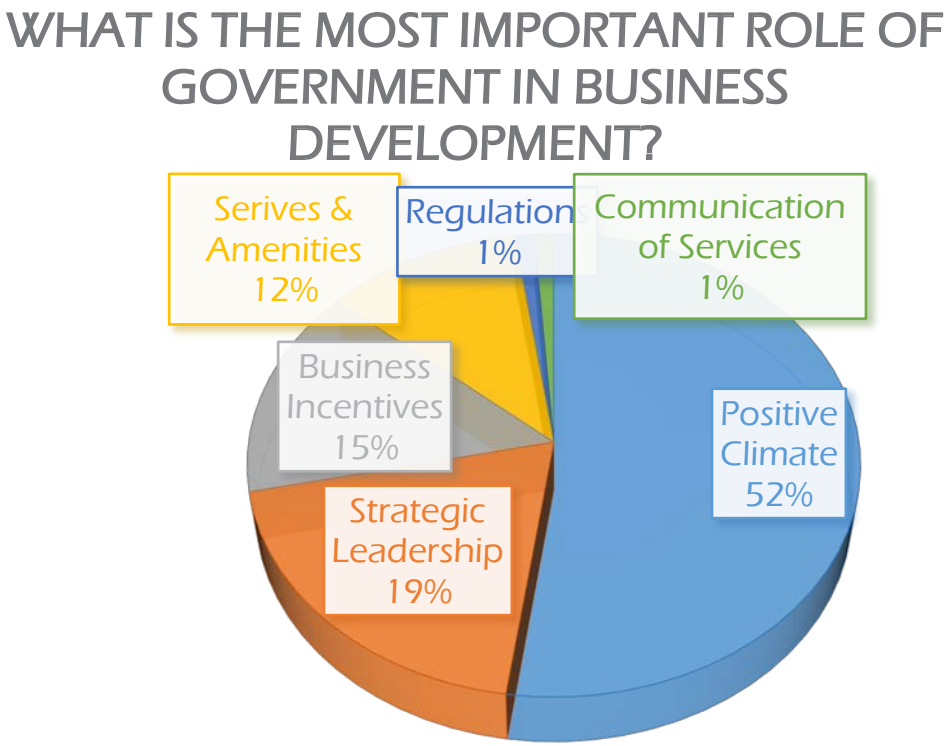
Executive Summary

- **Research Conducted**
  - The Economic Development Working Group referred to several resources related to the economic impact and projections of cybersecurity employment and corporate growth projections, including a 2017 internal report commissioned by the Indiana Economic Development Corporation (IEDC), comparisons with other state's indicated initiatives (e.g., GA, MI, MD, KY), employment data reported by US Department of Labor, Office of Economic Adjustment, and Emsi Occupation Snapshot Report for Q4 2017 (central Indiana).
  - The internal 2017 IEDC report is the result of a year-long investigation into the State's existing assets, needs of the private and public sector, opportunities for talent and commercial growth, and "threats" related to other states' strategic initiatives in the economic development of cybersecurity in their respective states.

- **Research Findings**
  - Our review of the economic development strengths, weaknesses, opportunities and threats (SWOT) of cybersecurity led the group to the following conclusions:
    - Cybersecurity should not be thought of as a discrete sector. Rather, all companies must have a cybersecurity awareness and plan in order to win and, in some cases, to even compete for business opportunities.
    - Cybersecurity is the fastest growing area within the technology sector. The global cybersecurity market has grown roughly 35x over 13 years to $120 billion in 2017.
    - Industry experts predict that growth will continue 8-15% each year for the next five years, meaning global spending on cybersecurity products will be >$1 trillion in the same period.
    - There is no standard definition of "cybersecurity," so collecting and tracking data for employment and economic development can be very challenging.
    - Indiana's largest assets are Academia and Innovation & Entrepreneurship (per IEDC report found in supporting documentation section).
    - Indiana's largest challenges are Workforce and Awareness / Communications (per IEDC report).
    - 267 discrete companies in the Indianapolis-Carmel-Anderson area competed to hire Cyber Analysts in the last year.
  - These conclusions led the working group to establish a preliminary declaration of its group ethos and mission that reads as follows**:**
    - Indiana's vibrant economy is based on a secure, stable environment. Today, in addition to physical security and fiscal stability, individuals and companies must be able to rely on cybersecurity to grow, invest, and prosper.
  - Economic development is advanced by:
    - Attracting and growing companies in all sectors by demonstrating Indiana's technical infrastructure readiness, backed by its commitment to safeguard that infrastructure;
    - Encouraging collaboration amongst companies and institutions on information protection strategies; and

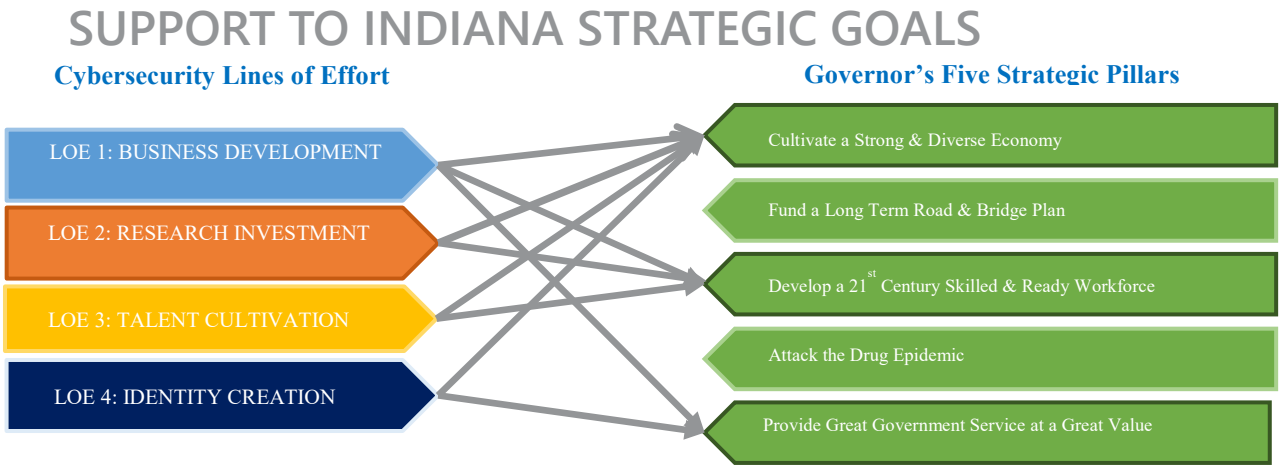
        - Considering and proposing policy recommendations to (a) support the attraction and growth and (b) promote further growth of existing cybersecurity companies.
    - Economic success is defined through both qualitative and quantitative metrics that focus on:
        - New business starts and attractions
        - Support to new start-ups
        - Retention of existing businesses
        - Number of new cybersecurity jobs created
        - Number of non-cyber jobs created to support new cyber business
        - Average salary of jobs created
        - New employee demographics (workforce diversity, education levels, etc.)
        - Retention of cybersecurity professionals who graduate from one of the State's universities or colleges, who accept Indiana-based cyber employment

- **Additional Findings**
    - Among several data, one important finding during the working group's research showed that Hoosier's believe the most important role of government in cybersecurity business development is positive economic climate, strategic leadership, and business incentives:



- **Committee Deliverables**
  - Incentive Program
  - Implementation Plan for Cybersecurity – Marketing
  - Cybersecurity SIoT Innovation District

- **Additional Notes / Way Ahead:**
  - The Economic Development working group will consider the following strategy and make recommendations around at least four discrete lines of effort that align to the Governor's Five Strategic Pillars:



- **References**

  - IEDC Cyber Initiative 2017
  - Ross, Alec. "Want job security? Try online security." Wired, April 25, 2016.
  - Morgan, Steve. Cybersecurity Market Report, Q1 2017. http://cybersecurityventures.com/cybersecurity-market-report/
  - Canales, Christian, R. Contu, S. Despande, E. Kim, L. Pingree. Forecast Analysis: Information Security, Worldwide, 2Q15 Update, Gartner, September 08, 2015.
  - Turnaround and transformation in cybersecurity: Key findings from the Global State of Information Security® Survey 2016. PwC, www.pwc.com/gsiss.
  - Morgan, Steve. Cybersecurity Market Report, Q1 2017. http://cybersecurityventures.com/cybersecurity-market-report/
  - Emsi Occupational Snapshot Report, Q4 2017. www.economicmodeling.com
  - Cyberpoint Technology & Innovation Center proposal to City of Baltimore
  - "Uncharted: New Partners Team up as Georgia Stakes its Claim on Cyberleadership," Adam Stone, Government Technology, October/November 2017.
  - "Cyber Threat: Indiana's Call to Action," Anita Nerses (Raytheon), Inside Indiana Business, August 9, 2017.

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Local nonprofits have supported students with programs
        - Techpoint (XTERN, Tech Fellowship)
        - Nextech (K12 CS support)
    b. Local companies working with Apprentice University for internships
    c. Purdue Polytechnic High School formation
    d. Additional university accreditations and degree options in computer science
    e. ISSA and ISACA chapters remain active as well as Infragard
    f. Gov. Holcomb announces CS K12 requirements as part of Next Level agenda
    g. IN-ISAC employs and trains Purdue students to monitor the State's network

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Small and Medium sized businesses
    b. Small local government entities (schools included)
    c. Insufficient infrastructure
    d. Insufficient workforce

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Education / Awareness of threat, impact, and opportunity
    b. Workforce development/retention

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Defense Federal Acquisition Regulation Supplement (DFARS) compliance
    b. GDPR – European Union's General Data Protection Regulation
    c. National Institute of Standards and Technology (NIST)
    d. Health Insurance Portability and Accountability Act (HIPAA)

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Maryland / Baltimore and local cooperation with National Security Agency (NSA)
    b. Michigan Economic Development Corporation
    c. Georgia Cyber Innovation and Training Center
    d. Rhode Island Corporate Cybersecurity Initiative
    e. CyberCalifornia

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. IEDC Cyber Initiative 2017
    b. Cyberpoint Technology & Innovation Center proposal to City of Baltimore
    c. "Uncharted: New Partners Team up as Georgia Stakes its Claim on Cyberleadership," Adam Stone, Government Technology, October/November 2017.
    d. "Cyber Threat: Indiana's Call to Action," Anita Nerses (Raytheon), Inside Indiana Business, August 9, 2017.
    e. Kentucky State Research

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Public Private Partnership (P3) Investment in cybersecurity incubators and accelerators

8. **What does success look like for your area in one year, three years, and five years?**

	Year 1	Year 3	Year 5
New businesses starts and attractions	1	5	10
Support to new start-ups	P3 formed or identified	Innovation Center established	
Number of new cybersecurity jobs created	10	75	250
Average salary of jobs created	$90,000	$100,000	$110,000
Minority & Female Participation	>5%	>10%	>25%
Retention of cybersecurity professionals who graduate from one of the State's universities or colleges, who accept Indiana-based cyber employment	50	150	250

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. Need to define exactly what State wants to be in cyber (e.g., security of smart mobility, energy grid, defense, manufacturing, agtech, fintech, insurance tech, bio/health) to focus growth and allocation of resources.
    b. Public Service Announcements (PSA) for awareness
    c. Educate educators
    d. Cyber clubs K12 & track talent
    e. Identify current assets and capabilities better (e.g., INFRAGARD, Henry St. DHS)
    f. Publicize this Council and the effort
    g. Utilize and promote the Information Sharing and Analysis Center (ISAC) as a tool

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. Indiana-based cyber-focus companies
   - Cimtrak (software)
   - Pondurance (services)
   - Rook Security (software and services)
   - RADcube (consulting and implementation)

b. Cyber-focused companies with office in Indiana
   - Optiv (reseller and services)
   - Proofpoint (software)
   - Mako Group
   - Rofori

c. Companies that do cyber but not as the primary focus:
   - EY
   - PwC
   - KSM Consulting
   - Crowe
   - Raytheon
   - Vespa Group
   - Rolls Royce
   - Booz Allen Hamilton

d. Cybersecurity workforce – Lacks definition

11. What do we need to do to attract cyber companies to Indiana?

a. Recommended Policy and State government considerations:
   - What marketing or branding can be used to coalesce messaging? Digital Crossroads or Cyber Crossroads?
   - Can IN.GOV website note "Tech" or "Cyber" in tandem with Business and Agriculture
   - What would be the impact of eliminating or narrowing non-compete agreements

b. Recommended infrastructure investments:
   - Cybersecurity tech park / innovation center, which would include:
     - Sensitive Compartmented Information Facility (SCIF)
     - Co-work area
     - Accelerator aspect
     - Cyber-range
     - K-12 programming
     - Expanded 5G wireless
     - High-speed fiber
     - Small Cells
     - Resilient Grid (strategic location / control of battery and gen-sets for critical infrastructure)

c. Recommended incentives for consideration:
    - Tax incentives for companies that move into the state that can demonstrate compliance with NIST standards (theory: secure companies present less burden and risk to the public);
    - Tax incentives for purchasing products and services from state-based companies;
    - Must be Hoosier businesses to bid on state and local government cybersecurity products and service RFQs so long as products and service offerings are substantially similar to other commercially available options;
    - Tax deduction for companies that make or have made investments in their digital security structure
    - Subsidize cost of Small and Medium Business (SMB) use of IN-ISAC.
    - Cybersecurity Investment Incentive Tax Credit
        - "A refundable tax credit is available for a minimum investment of $25,000 in a qualified Maryland Cybersecurity Company (QMCC). The credit is claimed by the QMCC. The QMCC may be allowed a tax credit of up to 33% of an eligible investment, up to $250,000."
        - Note: Indiana's Venture Capital Investment Tax Credit (VCI) is 20% up to $1,000,000

12. What are your communication protocols in a cyber emergency?

a. N/A

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. Use NIST standards for definitions
b. Increase awareness and messaging of threat and opportunity

Deliverable: Incentive Program

Deliverable: Incentive Program

General Information

1. **What is the deliverable?**
    a. An incentive program to help Indiana businesses meet cybersecurity standards and to promote growth in the cyber industry in Indiana.
    b. Goals:
        i. Incentivize Indiana companies to make cybersecurity a priority
        ii. Reward the use of Indiana based vendors when improving cybersecurity posture
        iii. Promote attraction of businesses to the State by marketing Indiana companies for implementing these precautions
        iv. Advance Indiana as a thought-leader
        v. Increase readiness / resilience to cyberattacks at corporate and government levels

2. **What is the status of this deliverable?**
    a. In-progress 50%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. It is the goal of this working group initiative to create economic incentives directly correlated to the improvement of cybersecurity measures by Indiana companies. These incentives will be composed of the following two areas of impact:
        i. A cybersecurity readiness framework will be selected which will serve as a measure to ensure Indiana businesses achieve and maintain a fundamental level of cybersecurity preparedness. Our recommendation is that Indiana businesses receive an annual tax credit for each year they are able to show that they meet or exceed the requirements of this program, perhaps as validated by a third party certification. The ongoing nature of the incentive is designed to encourage Indiana businesses to continuously monitor and adjust their cybersecurity programs as well as raise awareness of cybersecurity needs and preventative measures.
        ii. To strengthen the growth of the Indiana cybersecurity service provider businesses, it is the recommendation of this working group that additional incentives be entertained to offset the costs associated with performing the annual analysis and remediation activities. If an Indiana company selects an Indiana cybersecurity services provider to help them perform the necessary cyber preparedness certification activities, they should receive either a tax credit or stipend to offset the cost of these efforts. This will encourage Indiana businesses to hire Indiana businesses and lead to greater business and partnership growth opportunities.

6. **What metric or measurement will be used to define success?**
    a. Success will be defined by an increasing number of companies who are able to certify their cybersecurity preparedness. The program will need to track the initial number of companies who are compliant and the percentage of these compared to the number of all companies in the state. These numbers will need to be kept on a year-over-year basis and account for new companies that begin in, or move to, Indiana as well as those which close their operations.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Any business in Indiana that maintains some digital presence and thus is in need of best cybersecurity practices could benefit from this plan from two aspects. First, they would be eligible to receive a tax incentive and secondly, they would have a more secure cyber posture. In addition, cybersecurity professionals would benefit as there would be an increase in job opportunities as more businesses join the program. Even though the tax incentives themselves target businesses that would need cybersecurity, the entire business ecosystem of Indiana would benefit from a more secure operating environment as well as increased confidence in cybersecurity by existing and potential Indiana businesses.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Existing tax incentives for economic development. Existing tax credits that are available to businesses.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Possibly Policy

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Working with the IEDC and Department of Revenue to build upon existing incentive plans.

12. **Who should be main lead of this deliverable?**
    a. David Roberts

13. **What are the expected challenges to completing this deliverable?**
    a. Identifying valuations of various tax credits, calculating the direct return on investment for the state of these incentives and marketing the existence of the incentives as a way to attract new businesses and retain existing businesses.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Generate List of Possible Incentives	ED committee	100%	4/17/2018	See Appendix A
Research other economic development policies passed in other states regarding cybersecurity	ED and policy Committee	0%	February 2019	
Research other successful business incentive programs implemented by Indiana state agencies	ED committee	0%	February 2019	
Meet with IEDC policy director and further discuss possible incentives programs or policy	ED committee	0%	February 2019	
Put together recommendation to present to IECC	ED Committee	0%	March/April 2019	
Develop next steps for possible incentives per IECC feedback	ED Committee	0%	May 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
[N/A]					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. This initiative will encourage cybersecurity preparedness of Indiana companies. By incentivizing them to use Indiana companies for their cybersecurity improvements, we are encouraging intra-state business growth and partnerships. This will foster organic growth of our supply base.

18. How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?

a. By incentivizing businesses to meet varying levels of requirements, we will encourage them to do more than just meet the bare minimum requirements and provide an escalating path of greater security leading to greater incentives.
b. Depending on which incentives are agreed upon, there could be administrative overhead to monitor the program, validate findings, etc.

19. What is the risk or cost of not completing this deliverable?

a. By not directly incentivizing improvements in the cybersecurity posture of Indiana businesses, the State is not providing sufficient guidance of what are the appropriate security measures a company should strive to implement and potentially allow cybersecurity improvements to be an afterthought for companies who may be more financially focused or motivated.
b. A fragmented or ineffective legislative structure could also result.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. This may be the most challenging piece of this program. There are many frameworks available, but not all companies must subscribe to the same ones. Therefore, it may prove difficult to make direct comparisons across industries. Additionally, we do not propose placing an auditing requirement on State personnel. Therefore, this program would need to be based on self-reporting. Thus, a baseline may have to be established in year one of the program to identify current state with small incentives to report with larger incentives in year two of the program for those who self-reported in year one.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No
b. **If Yes, please list states/jurisdictions**
    i. We have not seen other states implement this yet, but have seen encouragement from the federal level which aligns with one of our recommendations of considering the NIST Cybersecurity Framework.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. Further research will be needed to validate the answer to Question #9 above. This research would then also identify potential jurisdictions that could be used as a control.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. No common definition of acceptable cybersecurity measures and several frameworks and models on which to base this program could lead to time-consuming discussions and debate.
b. The desire of this subcommittee to not require audits and rely on self-reporting which may not prove to be reliable.
c. Reaching consensus from policy makers.
d. Not enough money to fund the incentives.
    - Incentives need to tie to the potential for economic growth and the associated revenue creation.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    - Regulation and policy may be required to create and enable the incentive program.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. N/A

27. Can this deliverable be used by other sectors?

a. Yes

b. **If Yes, please list sectors**

- There could be potential overlap with the Workforce Development Committee with incentives around training and implementing these security components.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Not known

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Marketing to other states that Indiana takes cybersecurity seriously could have a potential benefit to our business attraction programs. This is a clear message to allow other companies to understand the preventative measures certified Indiana companies have taken and could influence other companies in their decision-making processes to do business with certified Indiana companies. It could also be a decision point when external companies are looking to move to the State as it increases the cybersecurity maturity of the companies with whom they will become associated.

List of Possible Incentives

- Annual tax credit for meeting / exceeding (complying) with cybersecurity preparedness standard
  - Consider increasing the credit for ongoing compliance?
- Incent through credits or deductions expenditures with Indiana companies supplying goods or services to incent organic supply base growth
- Provide training grants (possible scope: executives, technologists, general cyber hygiene to employees)
- Make VCI tax credit program transferrable to incent investment from other states into Indiana firms
- Create list of firms meeting certain requirements for supplying to State (i.e. "trusted" supplier list)
- Create incentive (e.g., tax deduction) for proof of cyber insurance coverage
- Direct tax credit for Indiana-based cybersecurity firms

Evaluation Methodology

Objective 1: IECC Economic Development Committee will propose a list of possible incentive programs to be considered by the State of Indiana by April 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: State of Indiana will establish an incentive program in Indiana by July 2020.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Implementation Plan for Cybersecurity - Marketing

Deliverable: Implementation Plan for Cybersecurity - Marketing

General Information

1. **What is the deliverable?**
    a. A comprehensive marketing plan to promote awareness and preparedness by Indiana citizens, governmental organizations, and businesses for cybersecurity, as well as promote Indiana's leadership in cyber.

2. **What is the status of this deliverable?**
    a. In-progress; 25% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☒ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Indiana has the opportunity to begin a marketing campaign surrounding cybersecurity and technology more generally in the state. Highlighting the big business deals such as the Salesforce purchase of ExactTarget and HomeAdvisor's merge with Angie's List would be part of the broader theme of a tech marketing campaign, as well as highlighting the vibrant startup community and available novel resources such public-private partnership and innovation resources. The campaign could focus on Indiana universities such as Purdue, IU, Notre Dame, Rose Hulman, Butler and more to show the quality of the talent pipeline in tech. The campaign could also highlight some of the cybersecurity work happening in Indiana, especially noting the intersection and influence on traditionally non-cyber places and applications such as 16 tech (e.g. Bio Sciences) and health organizations across the state. This campaign could also focus on a cybersecurity conference. Also, at a fundamental level, the campaign could be designed to raise awareness of citizens and businesses to the issues around cyber, good cyber hygiene, and opportunities for working in cybersecurity.

6. **What metric or measurement will be used to define success?**
    a. The best indicator of success will be increased awareness of State programs and interactions with out-of-state cybersecurity influencers. Another key indicator of success would be attracting a cybersecurity-related conference to Indianapolis.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. The State of Indiana as a whole will benefit from marketing that highlights the quality of cybersecurity available in the state and general need for good hygiene and compliance. Any new businesses considering a relocation or start in Indiana might be influenced by the strength of the marketing campaign. Existing business would benefit from more opportunity to highlight the great work that is being done around the state. Universities could leverage marketing efforts to attract and retain more out of state students interested in a career in cybersecurity.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Existing tourism-related efforts.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Will determine at a later date

11. Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?

a. Tourism, Visit Indy (https://www.visitindy.com/).

12. Who should be main lead of this deliverable?

a. Dave Roberts for IEDC, Matt Wade for Marketing

13. What are the expected challenges to completing this deliverable?

a. Many cities and locales are competing in this area. Standing out of the crowd will be difficult for a non-traditional cybersecurity locale such as Indianapolis.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. One-time deliverable (2-year initiative)

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Generate list of highlights	ED Subcommittee	100%	April 17, 2018	
Communicate with IEDC Marketing for execution plan	ED Subcommittee	10%	December 2018	
Present comprehensive marketing plan	ED Subcommittee	0%	August 2019	
Implement Marketing Plan	IEDC & 3rd Party Marketing Firm	0%	2020	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. External marketing firm; $250,000 for a 12-month campaign.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. This deliverable will provide the voice of market input to the State regarding suggested marketing strategy and tactics. Implementation of the recommendations will not be within the scope of this deliverable, as that function is best addressed by marketing divisions of state (IEDC) and local municipalities.

18. **How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?**
    a. Risk mitigation is achieved by increasing general public awareness, encouragement of growth in the sector, implementation of remedial and preventative measures by government and business, and promotion of proper cyber hygiene.

19. **What is the risk or cost of not completing this deliverable?**
    a. Based on available, current academia resources, Indiana education institutions may be utilizing fragmented, biased, and even incorrect information to teach the public about cybersecurity and the evolution of the state of Indiana.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Success is a list of specific, actionable, realistic marketing strategies to deploy.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. No
    b. **If Yes, please list states/jurisdictions**
        i. There is no known state-wide, comprehensive effort to market cybersecurity. Israel may have a similar example.

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. No

Other Implementation Factors

---

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable**?
    a. N/A

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. Recommendations from this subcommittee and others through the cyber community are needed for the strategies to remain timely.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. We have reached out to Marketing at IEDC

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. It can; however, a completed playbook should not be provided to other states at this time.

30. What are other public relations and/or marketing considerations to be noted?

a. This list should emphasize cyber-related events and updates that are projected to become the most impactful strategy going forward.

Evaluation Methodology

Objective 1: Indiana Economic Development Corporation will develop a 2-year marketing plan focusing on economic development and Indiana's cybersecurity posture by August 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indiana Economic Development Corporation will execute a 2-year marketing plan focusing on economic development and Indiana's cybersecurity posture in 2020.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cybersecurity SIoT Innovation District

Deliverable: Cybersecurity SIoT Innovation District

General Information

1. **What is the deliverable?**
    a. A strategic business plan for an innovation district designed to foster development and application of cybersecurity solutions; education and training; cross-collaboration among and between the private and public sector; and provide common resources to the industry in a setting managed by a public-private partnership model.

2. **What is the status of this deliverable?**
    a. In-progress; 50% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☒ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Indiana has the opportunity to establish, with the help of other public and private sector partners, at least one cyber innovation district. The goal of such a district or facility would be to provide the base-line assets necessary to facilitate innovation and collaboration in the cyber sector. The desired results would include (a) better access to the infrastructure for innovation for young or smaller cyber companies; (b) better collaboration between companies, both those in the cyber sector and with those outside the sector as they can find consulting services more readily; (c) improved collaboration between academia and the private sector; (d) access for government to combined goods and services; and (e) increased business and Intellectual Property (IP) growth around the cyber sector. Additionally, multiple districts or facilities could be established to focus on military as well as non-military concerns.

6. **What metric or measurement will be used to define success?**
    a. The goal is an identifiable project or multiple projects that includes a plan to execute the establishment of such a cyber innovation district or facility.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. The State of Indiana as a whole will benefit from the presence of one or more innovation districts, in much the same way that the state has benefitted from public-private partnerships of Indiana Biosciences Research Institute (IBRI) and Battery Innovation Center (BIC) in the biotech and energy sectors, respectively. Companies, both new and established, as well as academia, may also benefit, as would the military and defense sector.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. There are currently a few other states that have announced/started such initiatives, such as Maryland and Georgia, as well as some private assets within the State, but no current innovation district exists in the State.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Defense

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Office of Defense Development (IODD) and Indiana Office of Technology (IOT)

12. Who should be main lead of this deliverable?

a. Doug Rapp

13. What are the expected challenges to completing this deliverable?

a. Various stakeholders will have input on the features of this project, so harmonizing all interests will be a challenge. One strategy will be to start with a baseline, and they identify how multiple districts or facilities can address the varying interests.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Define goals and objectives of CSIoT District	ED Subcommittee	100%	May 17, 2018	
Identify Components, Features, & Services	ED Subcommittee	80%	September 30, 2018	
Outreach campaign to interested parties	ED Subcommittee	50%	December 31, 2018	
Review of data	ED Subcommittee	0%	February 2019	
Complete white paper / business plan	ED Subcommittee	0%	April 2019	
Submit recommendations to the council	ED Subcommittee	0%	August 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. This deliverable, if acted upon by the State of Indiana, will create significant economic growth through innovation, access to solution, and workforce. Further, it will regionally anchor the industry and become a draw for businesses from outside of Indiana.

b. Successful examples of cybersecurity ecosystems are Atlanta where two enterprise cybersecurity partners spun off over 200 cybersecurity start-ups/companies. Also, CyberSpark in Beer Sheva, Israel which has gained a world reputation for cybersecurity innovation through its unique partnerships between academia, government, the military, and the private sector. Currently, Israel is the second largest exporter of cybersecurity products, next to the U.S., in the world with exports 35 times their size.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will contribute greatly to risk reduction through emerging technology, access to solutions for both the public and private sectors, and an increased awareness of cybersecurity risks.

19. What is the risk or cost of not completing this deliverable?

a. Indiana misses the opportunity to establish itself within a high growth industry, which is the fastest growing sector in technology, and continued losses to the Indiana economy through cybersecurity incidents such as breaches and ransomware.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success is an identifiable project or multiple projects that includes a plan to execute the establishment of such a cyber innovation district or facility.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes

b. **If Yes, please list states/jurisdictions**

   i. Successful examples of cybersecurity ecosystems include Atlanta where two enterprise cybersecurity partners spun off over 200 cybersecurity start-ups/companies. Additionally, CyberSpark in Beer Sheva, Israel has gained a world reputation for cybersecurity innovation through its unique partnerships between academia, government, the military, and the private sector. Currently, Israel is the second largest exporter of cybersecurity products, next to the U.S., in the world with exports 35 times their size.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. N/A

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Recommendations from this subcommittee will address sustainability in the final product.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. We will begin outreach as part of the deliverable. It will include outreach to all other subcommittees and potential partners.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No

30. What are other public relations and/or marketing considerations to be noted?

a. If Indiana chooses to accept any or all of the proposed recommendations, this would be an impactful announcement.

Evaluation Methodology

Objective 1: Economic Development Committee will develop business plan recommendations for first cybersecurity/Security in the Internet of Things (SIoT) innovation district by end of August 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: State establishes first cybersecurity/Security in the Internet of Things (SIoT) innovation district, provided appropriate funding source made available, by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Indiana Economic Development Corporation Cyber Initiative Report – 2017

Indiana Economic Development Corporation Cyber Initiative Report

2017

INDIANA ECONOMIC DEVELOPMENT CORPORATION

Indiana

A State that Works®

CYBER INITIATIVE

2017

Prepared by Douglass C. Rapp, CISM, for IEDC with special thanks to:

Nick Goodwin, *Chief Strategy Officer*, Indiana Department of Workforce Development

Walter Grudzinski, *Director of Information Security and Business Continuity*, Vectren Corporation

Brandt Hershman, *State Senator, District 7*, Indiana Senate

Christopher Judy, *Representative, District 83*, Indiana House of Representatives

David Lefever, *Chief Executive Officer*, The Mako Group

Steve Lodin, *Senior Director of Cyber Security Operations*, Sallie Mae

Chetrice Mosley, *Indiana Cybersecurity Program Director*, Indiana Office of Technology and Indiana Department of Homeland Security

Chad Pittman, *Vice President of the Office of Technology Commercialization*, Purdue Research Foundation

Joel Rasmus, *Managing Director*, CERIAS at Purdue University

Leon Ravenna, *Chief Information Security Officer*, KAR Auctions

Stephen E. Reynolds, *Partner, Data Security and Privacy Practice*, Ice Miller Litigation Group

David Roberts, *President*, Battery Innovation Center

Dr. Eugene Spafford, *Executive Director Emeritus*, Purdue CERIAS

Nick Sturgeon, *IN-ISAC SOC Manager*, State of Indiana

Dr. Robert Templeman, *Senior Fellow*, Center for Applied Cybersecurity Research

J.J. Thompson, *Founder/Chief Executive Officer*, Rook Security

Tony Vespa, *Founder/Chief Executive Officer*, Vespa Group

Brad Wheeler, *Chief Information Officer*, Indiana University

THE OPPORTUNITY

The conditions for successful economic development in cybersecurity are incredibly strong in Indiana. Indiana possesses the right resources to become a driving force in the cybersecurity industry and emerge as a recognized world leader in cybersecurity research and innovation.

Indiana advantages include

- A strong talent pipeline stemming from over 50 colleges and universities
- A vibrant entrepreneurship/innovation culture
- A State Executive Counsel on Cybersecurity[1]
- World renowned research facilities and personnel
- A long history of pioneering innovation in the field
- A strong and collaborative cybersecurity community
- Unique military assets and businesses
- Expert training and exercises

Indiana needs only to foster the community and leverage existing strengths to achieve greater success.

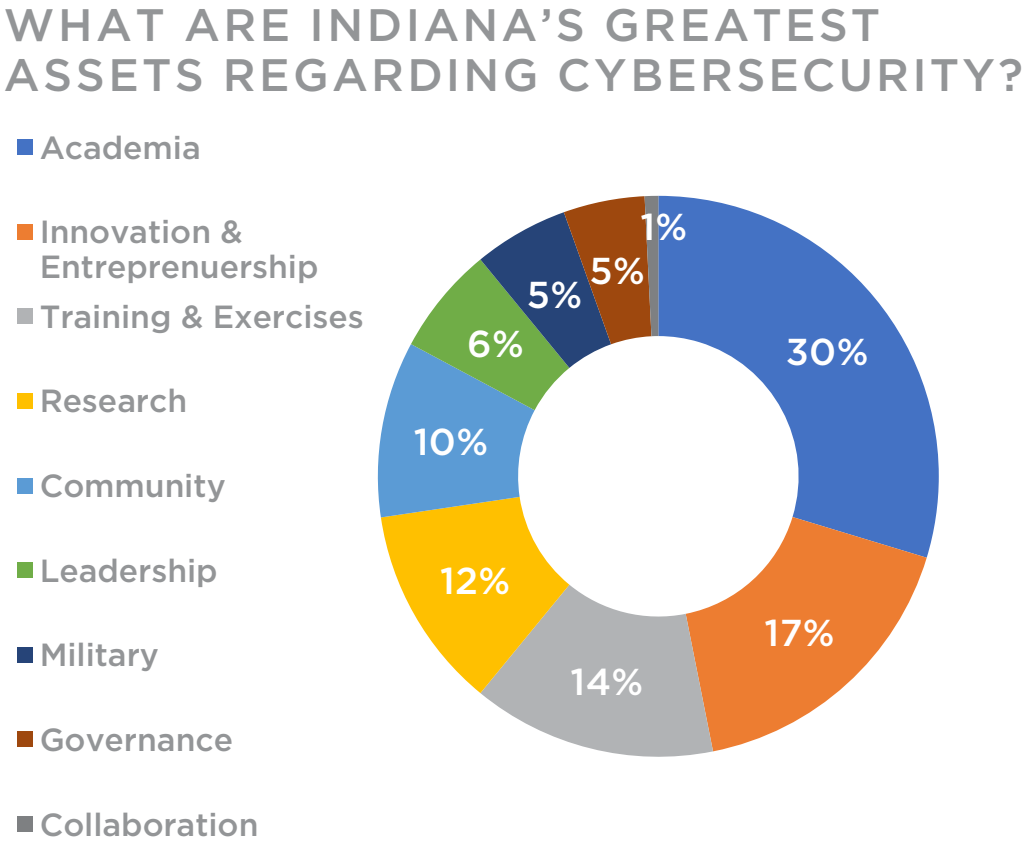


Figure 1. Indiana cybersecurity industry survey results on greatest assets.

[1] See Annex A: Executive Council on Cybersecurity

MARKET OVERVIEW

Cybersecurity is the fastest growing area within the technology sector and one of the fastest growing industries worldwide. The global cybersecurity market has grown roughly 35 times in 13 years going from $3.5 billion in 2004 to $120 billion in 2017[2] and industry experts predict that growth will continue 8-15% each year for the next five years. Global spending on cybersecurity products will eclipse a cumulative $1 trillion in the same period[3]. The market will continue to grow at a comparable rate to the growth of the Internet/Internet of Things.

To combat the ever-expanding number of threats and complexity of off-the-shelf attacks, companies are investing more than ever into Cybersecurity. Worldwide spending on cyber security reached $75.4 billion in 2015 and shows no sign of slowing[4]. The continued proliferation of cyber threats is driving so much spending on cyber security that it has become difficult for industry analysts to keep up. Industry surveys have indicated that respondents are increased their cybersecurity budgets roughly at an average of 24% in 2015[5] and show no signs of slowing down. Many businesses are spending much more. J.P. Morgan & Chase has doubled its budget to a record $500 million and Bank of America has stated publicly that they have no set budget– they will invest what it takes to secure their company. The U.S. Government has committed to a record 35% spending increase to $19 billion in 2017[6].

Challenges

Cybersecurity has only recently been recognized as a market. Research is complicated by the fact that it is neither a defined industry by the North American Industry Classification System (NAICS) nor the Standard Industrial Classification (SIC). Occupation codes by the Standard Occupational Classification (SOC) system are only now starting to be developed[7]. These codes are important because they are used by federal agencies such as the Bureau of Labor Statistics and Census Bureau to classify workers and employers in the vast amounts of public data they publish.

Contributing to industry confusion is the fact that there is no standard definition for cybersecurity, thus past and current reports rely heavily upon the reporter's individual definition and interpretation. A company that specializes in cybersecurity may currently be classified as a software firm, a consulting firm, or a security firm. Organizations routinely employing sizable cybersecurity staff include financial institutions, healthcare organizations, law firms, utilities, educational institutions, retail enterprises, and manufacturers yet are not necessarily considered in reports regarding the cybersecurity industry. A cybersecurity professional may be classified as an information security architect, computer network architect, security consultant, computer and information systems manager, or simply an "IT technician".

[2] Ross, Alec. "Want job security? Try online security". Wired, April 25, 2016.
[3] Morgan, Steve. Cybersecurity Market Report, Q1 2017. http://cybersecurityventures.com/cybersecurity-market-report/
[4] Canales, Christian, R. Contu, S. Despande, E. Kim, L. Pingree. Forecast Analysis: Information Security, Worldwide, 2Q15 Update, Gartner, September 08, 2015.
[5] Turnaround and transformation in cybersecurity: Key findings from the Global State of Information Security® Survey 2016. PwC, www.pwc.com/gsiss.
[6] Morgan, Steve. Cybersecurity Market Report, Q1 2017. http://cybersecurityventures.com/cybersecurity-market-report/
[7] There are currently no NAICS or SIC codes associated with the keywords cybersecurity or information security.

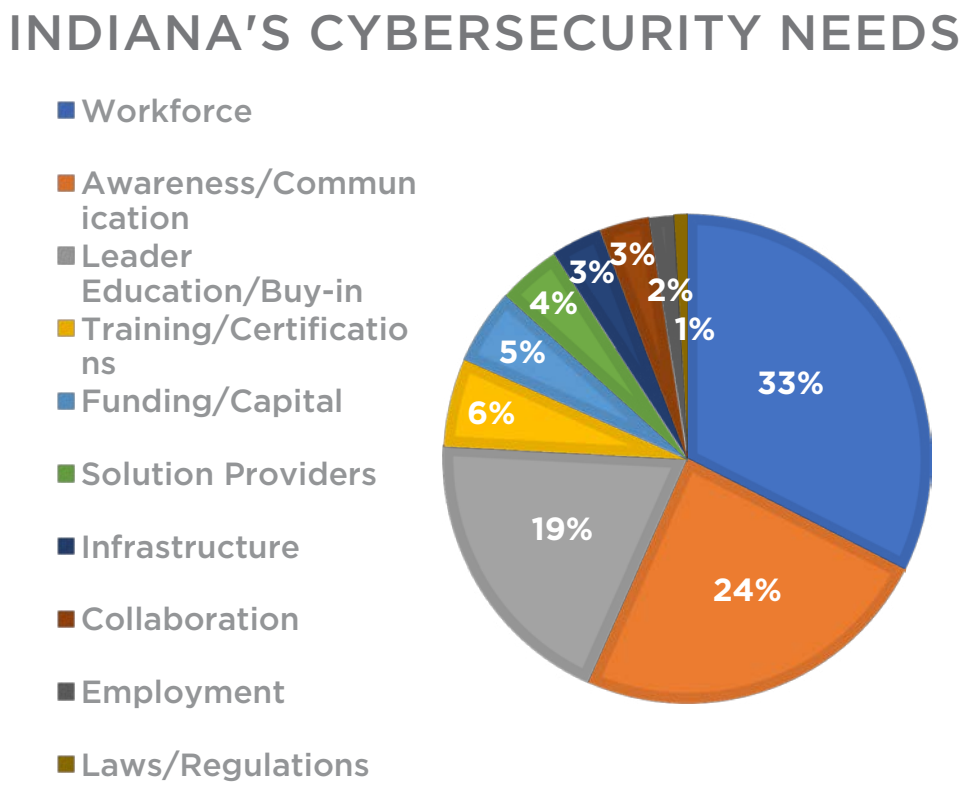


Figure 2. Indiana cybersecurity industry survey results on greatest cybersecurity needs.

Despite numerous advantages, Indiana faces several challenges that will need to be addressed for the State to achieve a dominant position in the marketplace and to accomplish strategic goals. According to a cyber security industry survey conducted by the Indiana Economic Development Corporation (IEDC)[8] in 2016-2017, Indiana challenges include:

- Attraction and retention of cybersecurity talent
- Access to funding/capital
- C-Suite/Executive level education and buy-in
- Increased local solution providers
- Investment in cybersecurity infrastructure
- Local access to training and certifications
- Increased collaboration through public/private partnerships (P3)
- On-going support of existing expertise and resources
- Cybersecurity awareness and communication

[8] See Annex B: Indiana Economic Development Corporation Cybersecurity Survey

The Goal

Indiana's continued economic success in the cybersecurity market lies in its core strengths of creating and applying things or being "a State that Works", its outstanding business climate, and willingness to embrace technology and emerging markets.

Establish Indiana as a world leader in cybersecurity and the nucleus of cybersecurity in the region.

Success will be identified through both qualitative and quantitative metrics that focus on

1) The attraction of new businesses to the State
2) Support to new start-ups within the State
3) The retention of existing businesses within the State who may be exploring moves
4) The number of new cybersecurity jobs created
5) The number of non-cyber jobs created to support new cyber business
6) The salary of jobs created
7) New employee demographics (workforce diversity, education levels, etc.)
8) Lessening the "Brain-Drain" by increasing the number of cybersecurity professionals who graduate from one of the State's universities or colleges, who accept Indiana-based cyber employment

The Strategy

The strategy for Indiana economic development within cybersecurity is grounded in market research at the state, national, and international levels. Through research, industry engagement, asset inventory, and SWOT analysis, four strategic lines of effort were identified.

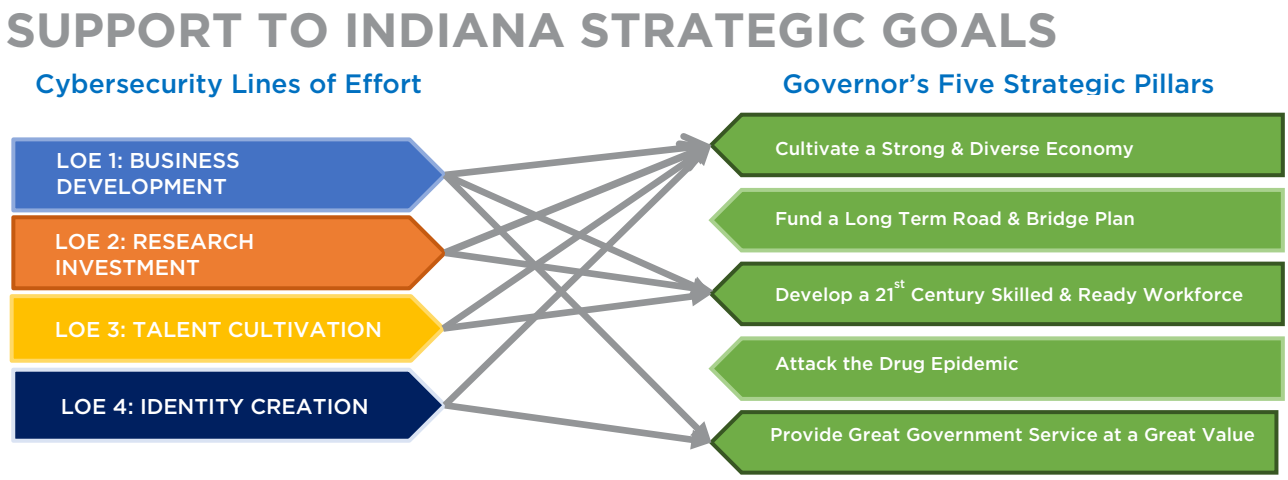


Figure 4. Cybersecurity lines of effort support to Indiana Strategic Goals

Line of Effort 1: Business Development

The business development line of effort (LOE) is rooted in the fundamentals of business development strategy.

- Business recruitment/attraction
- Business retention/expansion
- Business creation (innovation and entrepreneurship)
- Creativity and talent cultivation
- Place-making

The strategy will focus on defining and developing strategies/plans for industry clusters, developing a regional strategy/plan, creation of demand/retention of wealth, retaining and expanding cybersecurity businesses, leveraging existing military facilities and expertise, and investing in innovation and entrepreneurship.

Immediate progress can be made through investment into Indiana cyber companies with resources allocated under the State of Indiana's $1B innovation and entrepreneurship initiative and other tools. By doing so, Indiana will help relieve banking limitations caused by a lack of physical assets to secure lending[9], reduce risk associated with investors who don't understand cybersecurity, and reduce the barriers in attracting non-pillaging investment from out of state investors to fuel A and B round growth. Additionally, we can increase success of Indiana cybersecurity companies by adopting an "Indiana first" policy in State and local government.

Mid- and long-term strategies for business attraction will focus on large cybersecurity company relocation, and on attracting research and development offices from big companies that are not ready to relocate to Indiana. We will create an environment to unlock intellectual property from these companies that will seed synergistic industry clusters through start-ups[10].

Line of Effort 2: Research Investment

Research and development drives economic growth. These activities allow researchers and scientists to develop and apply new knowledge, techniques, and technologies. As technology evolves, productivity increases and businesses can produce more with fewer resources. Indiana is home to three prominent R1 universities (Indiana University/Bloomington, Notre Dame University and Purdue University/West Lafayette) who have major R&D initiatives in cybersecurity, but active and productive cyber research is also conducted at several other Indiana schools, including Ball State, Indiana State University, Indiana University–Purdue University at Indianapolis, Indiana–Purdue University Fort Wayne and Purdue University/Calumet. Five NSA/DHS Centers for Academic Excellence are headquartered at Indiana-based institutions of higher education.

[9] Traditional company valuation relied on heavily on physical assets. As newer business models evolve, investors are beginning to recognize services, technology creation, and network orchestration as important components in determining value.
[10] Sometimes referred to as a "Cluster Effect". An example of this is the 45+ information security companies that emerged from Internet Security System and SecureIT in Atlanta, GA.

"Leading in cybersecurity requires fast-paced innovation in technology, policy, and practice. Indiana has the deep strengths in its research universities, partnerships, and workforce for firms to thrive in the heartland."
Brad Wheeler, CIO, Indiana University

The strategy in this line of effort will concentrate on

- Support to research consortiums
- Increase contracting capacity to government
- Establish a presence in both national and international strategic markets
- Foster collaboration on grant writing/funding efforts
- Make clear, visible commitments to people and institutions in the field

Line of Effort 3: Talent Cultivation

Cybersecurity is experiencing a significant shortage of practitioners. Conservative estimates indicate over a quarter-million positions currently sit unfilled in the US alone, and a shortage of 1.5 million cybersecurity professionals is predicted by 2019[11]. The ability to produce and retain cybersecurity talent will give Indiana a distinct market advantage. Indiana currently produces a significant number of cybersecurity professionals and possesses the assets to create more. Indiana advantages include:

- 30+ colleges and universities with specific cybersecurity/information security degrees, certificates programs, or course work[12]
- 72 schools in Indiana producing graduates with competencies related to becoming a Cyber Security Analyst over the last 5 years[13]
- 70+ middle and high school Cyber Patriot teams in Indiana[14]

The strategy for this line of effort will focus on collaborating with the Department of Workforce Development, academia, and industry to create a comprehensive cybersecurity talent pipeline strategy, incentives to attract/retain talent, utilizing data to strategically determine workforce needs, and supporting K-12 cybersecurity initiatives.

[11] Morgan, Steve. "Cybersecurity job market to suffer severe workforce shortage." CSO Online, July 2015, http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html
[12] Asset Inventory conducted by the Indiana Economic Development Corporation.
[13] Emsi Occupation Snapshot Report. Cyber Security Analyst in Indiana. Emsi Q1 2017 Data Set, www.economicmodeling.com
[14] List provided by Cyber Patriot.

"By far, our greatest assets in Indiana are the skilled talent we have access to. There are pockets of highly accomplished individuals who set the tone for the cyber environment in our state, and really the entire mid-west. This also holds true for the potential talent pool that is up and coming due to the dedication of State of Indiana's economic development initiatives."

David Lefever, Chief Executive Officer
The Mako Group

While there is a growing interest in cybersecurity at the 8-12 grade levels, few of Indiana's secondary education districts have relevant computer programming or cybersecurity programs.
An investment in middle and high school level educational initiatives could provide a dramatic payoff by influencing Indiana students to choose to pursue a cyber career path. While Indiana's colleges and universities are at the forefront of cyber education and research, many of its students are non-Indiana citizens who graduate and leave the state. An investment in grade 8-12 CS/Cyber programs would increase the number of future college-educated CS/Cyber professionals seeking career jobs in Indiana. IEDC should work with the Department of Education and the Department of Workforce Development to strengthen Indiana's commitment to preparing students for this growing, high-paying industry.

Understanding and enhancing the work-life culture that is important to the attraction and retention of cybersecurity talent will be a critical component of this LOE.

Line of Effort 4: Identity Creation

The State of Indiana has been very successful at branding itself as "The State That Works." Indiana has long since recognized the value of a strong brand identity. By synchronizing with the current brand campaign, Indiana will create a brand/identity for Indiana economic development efforts in cybersecurity. Key qualities and benefits this brand include:

- Indiana is a State that creates and applies cybersecurity (a "State that Protects")
- Indiana is a state that understands and excels in collaboration between government, academia, and private industry
- Indiana is a State that welcomes and recognizes the value of diversity
- Indiana's business environment creates a competitive advantage for our businesses
- Indiana is a great place to live, work, and play

By synchronizing this messaging and branding strategy within the Indiana cybersecurity sector, Indiana will illustrate a comprehensive approach to demonstrating benefit. Indiana will strategically target regionally (Midwestern states with an economic climate that is less business-friendly than Indiana), nationally and internationally, and leverage relationships with industry, academia, and the military to expand opportunities.

"Driving economic development by bringing together resources from top flight schools, state government and business is but one benefit in the fight against cyber criminals that can impact every person and business. That's what Indiana does!"

Leon Ravenna, Chief Information Security Officer
KAR Auctions

IMPLEMENTATION

Line of Effort 1: Business Development

1.1 Cluster Strategy: Services, Forensics, ICS/SCADA, SIoT (Manufacturing integrity/Sensors)

Managed Security Services

Cybercrime continues to drive the consumer cybersecurity market and high growth areas in managed security services are predicted to be analytics/SIEM (10%); threat intelligence (10%); mobile security (18%); and cloud security (50%)[15]. It is imperative that Indiana attracts, nurtures and sustains companies and offers initiatives that foster cybersecurity solutions for small to midsize businesses as they historically have been the most vulnerable and generated the most risk.

Digital Forensics

The global digital forensics market was worth $2 billion in 2014 and is predicted to reach $4.9 billion by 2021. Market growth is projected to be 12.5% CAGR from 2015 to 2021[16]. Indiana has numerous unique assets in digital forensics including Purdue University's internationally lauded Cyber Forensics Laboratory and a high concentration of digital forensic expertise within the Indiana State Police and other entities.

Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA)

Increasing attacks on critical infrastructure such as power, water, oil and gas, manufacturing, transportation, and others is the major force driving the ICS security market. The Industrial Control Systems (ICS) security market size is estimated to grow from $9 billion in 2016 to $12.6 billion by 2021, at a Compound Annual Growth Rate

[15] IDC Report. http://www.idc.com/
[16] Digital Forensics Market - Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2016 – 2026. Transparency Market Research, July 30, 2015, http://www.transparencymarketresearch.com/digital-forensics-market.html

(CAGR) of 7%[17]. With Indiana leading the nation in manufacturing job growth -- home to both the second largest automotive industry in the nation
and unique capability facilities such as the Muscatatuck Urban Training Center (MUTC) —Indiana has the environment to increase innovation and its leadership within this market segment.

Securing the Internet of Things (SIoT)

IoT security is continually evolving and is ~~both~~ the responsibility of both the government and the private sector. Indiana's chief roles in the SIoT is to provide tools and resources to businesses that incorporate security into product development, improve security to consumer and vendor-managed devices, and secure the infrastructure that enables these devices. Serving as a catalyst for SIoT efforts in Indiana are the research at Indiana University School of Informatics and Computing, at Purdue's CERIAS, and the high level of expertise Crane Naval Surface Warefare Center.

1.1.1. Action: The IEDC needs to create cluster organizations and solicit cybersecurity action plans by convening economic development entities, industry, academia, military, and innovation/entrepreneurship leaders. Plans should be solicited by region (regional cities) and should be competitive for State resources.

1.2 Create a community and communicate efforts.

1.2.1. Action: Indiana needs an industry organization to organize cluster activity, assist the IEDC in execution of the Strategic Cybersecurity Economic Development Plan, partner with both IEDC and DWD on synchronizing talent development activities, represent industry interests, create and execute industry events, and disseminate industry information.

1.2.2. Action: Indiana needs to build a significant cybersecurity conference that showcases existing talents and assets within the State. This event should be industry driven but supported by the State.

[17] Industrial Control Systems (ICS) Security Market by IT Solution, by IT Service (Risk Management Services, Design, Integration and Consulting, Managed Services, and Audit and Reporting), by Vertical & by Region - Global Forecast to 2021. marketsandmarkets.com, July 2016.

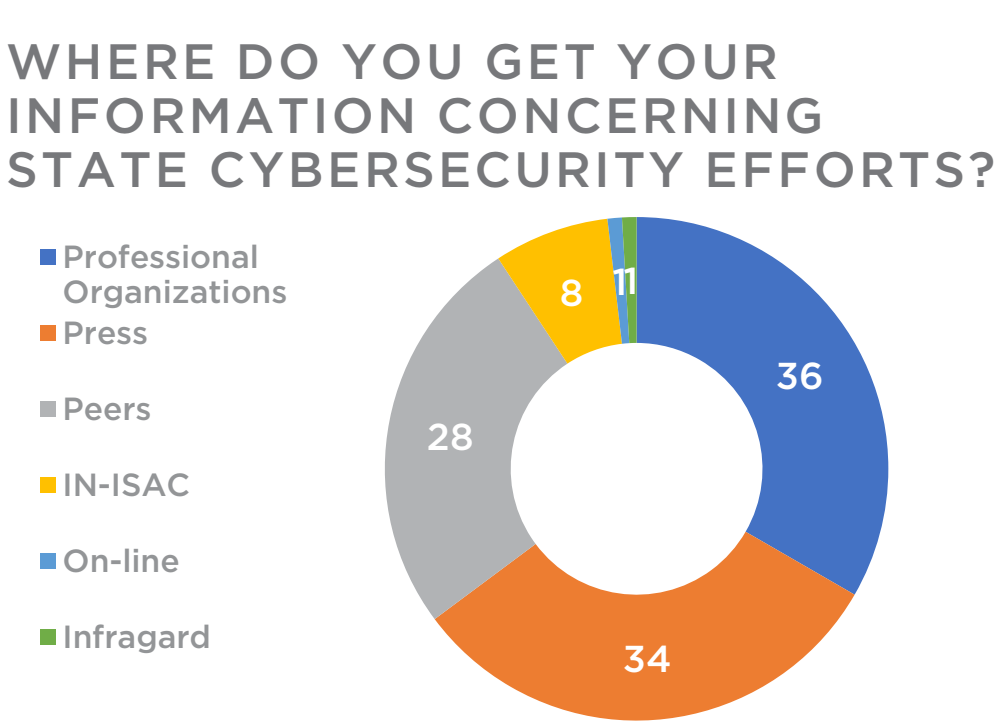


Figure 5. Indiana cybersecurity industry survey results on State information.

1.3 Create Demand/Retain Wealth

1.3.1 Action: Invest in a resource center that provides security solutions to our most vulnerable businesses. According to the National Small Business Association, Indiana small businesses employ 45.5% of our workforce[18]. Small business is the most susceptible business sector to cybercrime as they generally cannot afford to in-house cybersecurity talent and there are fewer providers that offer affordable scaled solutions. Studies have indicated that up to 60% of small business fail within 6 months of a significant cyber incident such as a breach or ransomware[19]. Coupled with the cost of complying with rising information security requirements mandated
in regulations such as Defense Federal Acquisition Regulation Supplement (DFARS), the European Union's General Data Protection Regulation (GDPR) and others, many business
are accepting risk of and transferring that risk to everyone that they do business with.

Indiana should invest resources available from government, academia, and the private sector
to form P3 entities which specifically address the risk to small and mid-sized business. Indiana should fuel demand by educating businesses on vulnerabilities and secure wealth by mitigating costs associated with cybersecurity incidents.

1.4 Innovation and Entrepreneurship

1.4.1. Action: Attract or create a cybersecurity accelerator with a proven business model to become self-sustaining[20]. The accelerator should have partnerships with both academia and private industry to unlock and transfer intellectual property to the market.

[18] Small Business Profile – Indiana. U.S. Small Business Administration, Office of Advocacy, 2017.
[19] National Cyber Security Alliance (NCSA) and Symantec Annual Survey, http://www.staysafeonline.org/stay-safe-online/resources/
[20] Accelerators should specifically be fixed-term, cohort-based programs that include formal educational and mentorship components, facilitate opportunity to access sufficient capital and culminate in public pitch or demo day. Examples
can be found at the Seed Accelerators Rankings Project at Rice's Jones Graduate School of Business.

1.5 International Strategy

1.5.1. Action: Create a formal research relationship with key countries (e.g., Israel, India, Singapore, and the "5-Eyes") and develop a strategic plan with quantifiable metrics for cybersecurity business development as part of a larger technology business development plan.

1.6 Regional cluster organization and action plan

1.6.1. Action: Create a formal consortium within the region through partnerships with Illinois, Ohio, Michigan and Northern Kentucky. Conduct a detailed asset inventory and an action plan for attracting cybersecurity talent and businesses to the Midwest to compete against other markets.

1.7 Leveraging Military Assets

1.7.1. Action: Unlock the potential of our statewide military assets by engaging elected and appointed officials to reduce regulatory barriers associated with private industry use. Invest in infrastructure at the Muscatatuck/Atterbury cyber physical range to attract private entity utilization. Invest in infrastructure at Westgate so that NSWC Crane can expand workforce into the technology park. Invest in and enhance infrastructure at Baer Field and Terre Haute Air National Guard Bases to leverage both intelligence and security operations center assets. Invest in other installations and assets as they are identified.

1.8 Identifying Factors Affecting Business Growth and Retention

1.8.1. Action: Determine other factors that would cause businesses to establish in states other than Indiana, and develop strategies to address them. This includes potential negative concerns (e.g., access to coasts, social issues, energy costs), and potential positive issues (cost of living, moderate climate). A plan should be formulated to enhance Indiana's positioning and image in these regards.

Line of Effort 2: Research Investment

2.1 Increase contracting capacity

2.1.1. Action: Support organizations in Indiana that are working to expand or create contracting capacity with priority going to those whose goal it is to leverage Indiana businesses and innovation through the creation of progressive tools such as Other Transaction Authorities. Priority should also be given to consortiums built around tools managed by Indiana entities
with minimal facility and administration (F & A) costs.

2.2 Support to research consortiums

2.2.1. Action: Support to cybersecurity research consortiums such as Center for Applied Cybersecurity Research (CACR) at Indiana University and the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University.

2.3 Establish a stronger presence in Washington, D.C.

2.3.1. Action: Establish a stronger presence in Washington, D.C. to engage the federal Cybersecurity community and facilitate the access of Indiana businesses to the $19B government cybersecurity market.

2.4 Grant Collaboration

2.4.1. Action: Establish leadership by developing grant writing talent that can attract

funding from federal sources specifically to support strategic initiatives contained in this plan.

Line of Effort 3: Talent Cultivation

3.1 Cybersecurity talent pipeline strategy.

3.1.1. Action: Support the Department of Workforce Development in utilizing data to strategically determine workforce needs and create a cybersecurity workforce pipeline. Synchronize efforts in research, marketing, and strategy within the cybersecurity sector.

3.2 Incentives to attract/retain talent.

3.2.1. Action: Engage State leadership to create a State Cybersecurity Scholarship. The scholarship could utilize existing education funds and provide ~~a~~ two-year scholarship ($25,000 per year) that stipulates the recipient's commitment to work in cybersecurity at the State or Indiana local government level for each year the scholarship is accepted[21].

3.2.2. Action: Engage State leadership to create individual tax incentives for cybersecurity professionals living in Indiana, a Federal security clearance cost tax credit, and other creative tools to attract and retain cyber security talent, businesses and research.

3.3 Support to K-12 cybersecurity programs.

3.3.1. Action: Create an organized state-wide cybersecurity competition incorporating other programs such as CyberPatriot and US Cyber Challenge. Establish regional and State level cyber camps leveraging industry organizations, universities, businesses, and military assets[22].

3.3.2 Action: Strengthen the State's K-12 CS/Cyber educational programs by providing grants to grade 8-12 public schools to implement state-approved CS/Cyber educational programs, and by offering train-the-trainer workshops for K-12 teachers. Offer a state-recognized basic cybersecurity certificate program to all high school students.

Line of Effort 4: Identity Creation

4.1 Collateral

4.1.1. Action: Create cybersecurity economic development web content, single page collateral, multiple page state asset collateral, and branding/display materials.

4.2 Targeted marketing plan

4.2.1. Action: Create a detailed marketing plan targeting cybersecurity businesses in the Washington D.C., Baltimore, San Francisco, New York, Boston, Chicago, Austin,

[21] CyberCorps Scholarship for Service (SFS) has a scholarship targeting federal information assurance professionals. Currently, only Purdue University participates in this program. The Commonwealth of Virginia created the Cybersecurity Public Service Scholarship Program however it is currently unfunded.

[22] Both CyberPatriot and US Cyber Challenge teams exist across the State of Indiana. Indiana should establish a program with camps that utilizes Indiana assets while incorporating teams from these existing programs.

and Atlanta[23]. The plan will be synchronized with other efforts in these geographic areas and will include advertising, industry events, and engagement opportunities.

FUNDING PLAN

Investment strategy for the Indiana Cybersecurity Economic Development Plan is based on core principles:

1. Incentives are tied to the strategic plan.
2. Resources are maximized through industry led initiatives, partnerships, and collaboration.
3. Incentives are performance based with claw back provisions.
4. Supported actions are evaluated on metrics of measured results and outcomes.
5. Supported actions are evaluated on quantitative or qualitative Return on Investment (ROI).
6. An economic and fiscal impact analysis will be conducted on projects as necessary.
7. A cost-benefit analysis will be conducted on projects as necessary.

[23] These cities are generally regarded as having a strong cybersecurity business sector.

Annex A: Executive Council on Cybersecurity

In April 2016, former Governor Mike Pence announced the formation of the Indiana State Executive Council on Cybersecurity (Cybersecurity Council), a comprehensive public-private partnership charged with enhancing Indiana's ability to prevent, respond to and recover from all types of cybersecurity issues, including attacks. The Cybersecurity Council, continued under Executive Order of current Governor Eric Holcomb, includes expertise from public and private partners.

The Cybersecurity Council's goals include formalizing strategic cybersecurity partnerships across the public and private sectors, strengthening best practices to protect information technology infrastructure, and building and maintaining robust statewide cyber incident response capabilities. Indiana is calling on experts in state and federal government, business, Indiana's National Guard, and academia to work together, communicate in a timely manner and share best practices for mitigating cybersecurity threats.

The Cybersecurity Council is currently comprised of 23 members from various public and private sector organizations across the state.

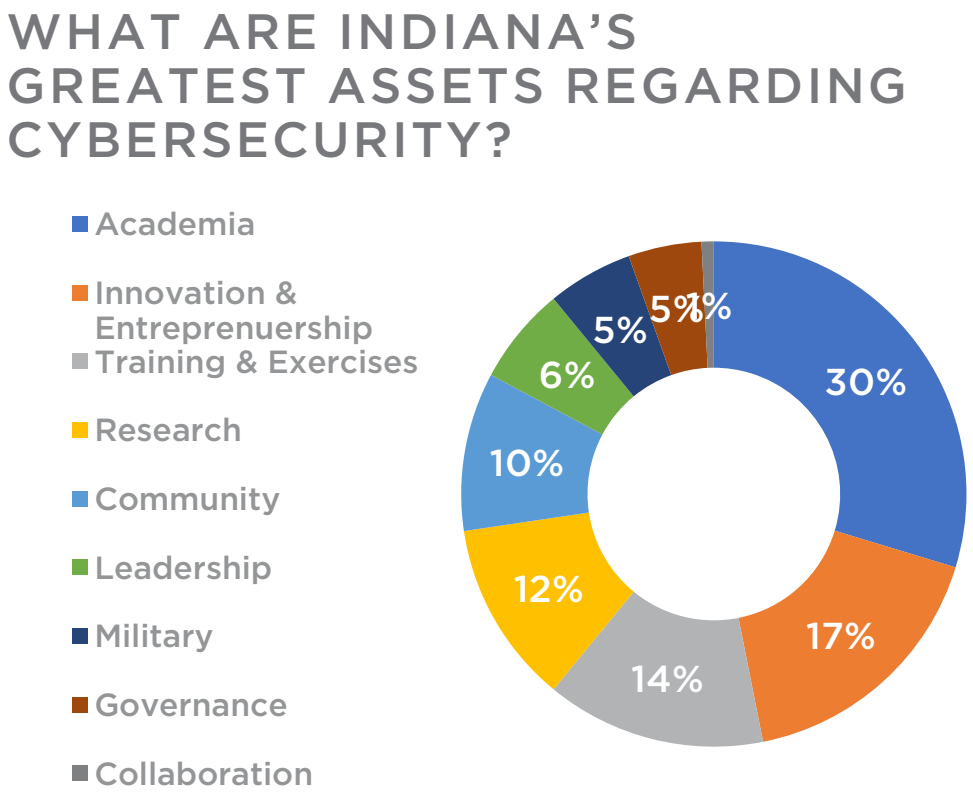
Current Executive Orders can be found at http://www.in.gov/gov/2384.htm.

Annex B: Indiana Economic Development Corporation Cybersecurity Survey

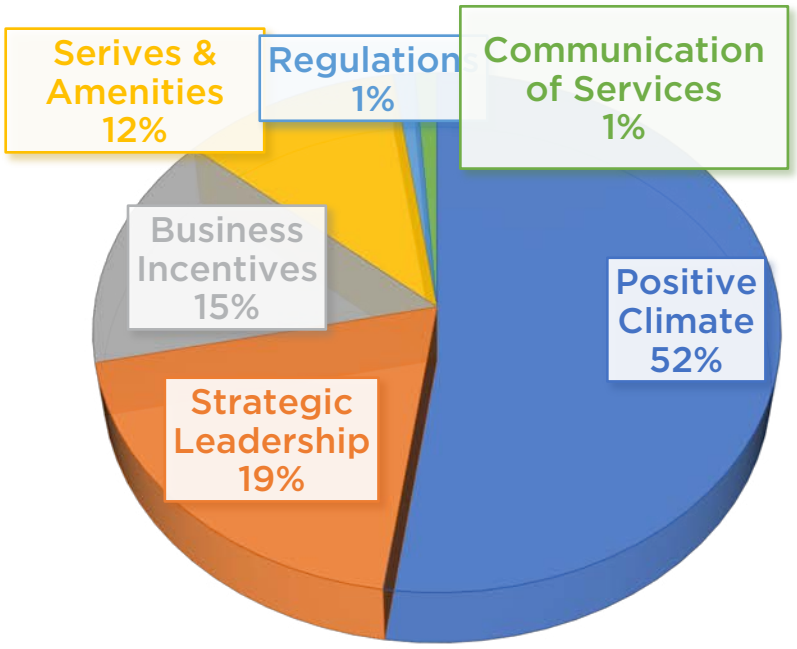
The IEDC developed and conducted a cybersecurity industry survey which was distributed in hard copy to participants of the Cybersecurity Town Halls as well as made available online. The purpose of the survey was to

- Determine what motivates and identify issues of concern and interest Indiana's cybersecurity community.
- Receive comments, opinions, and feedback on Indiana cybersecurity environment
- Discuss important topics/issues
- Facilitate an unbiased approach to the development of the Indiana Cybersecurity Economic Development plan
- Conduct an initial asset inventory
    - Create a benchmark to which future results can be compared

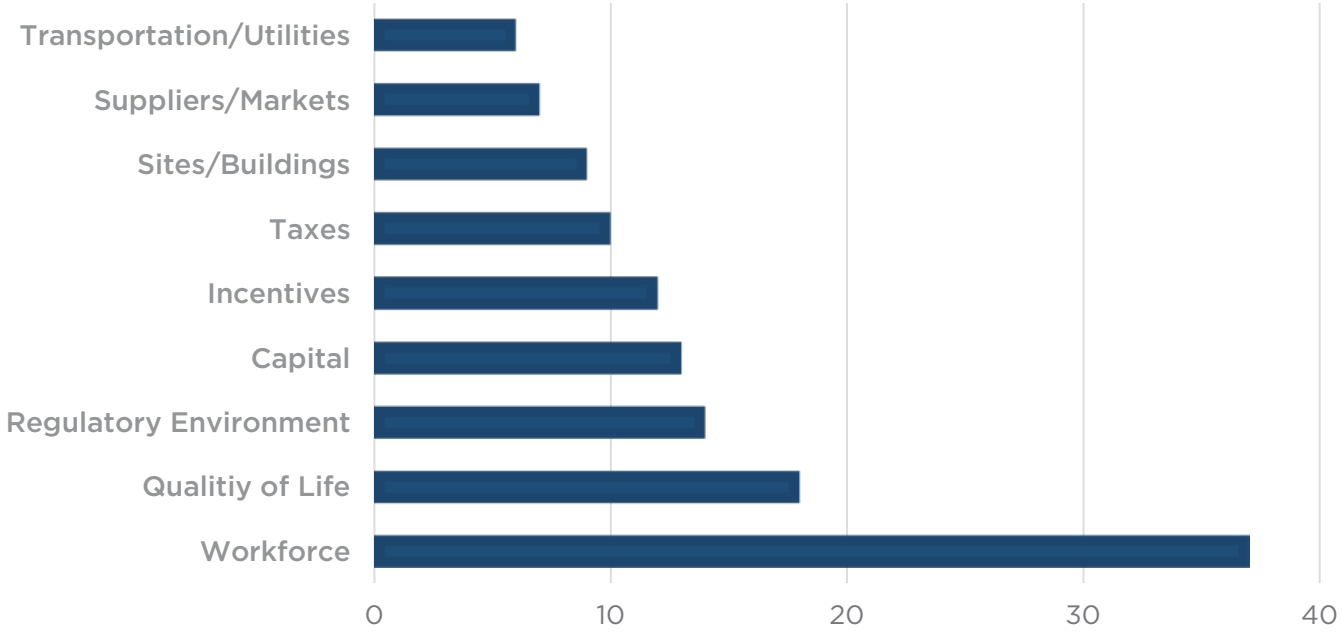
Highlights of the survey results that were key to the development of this plan are depicted below.



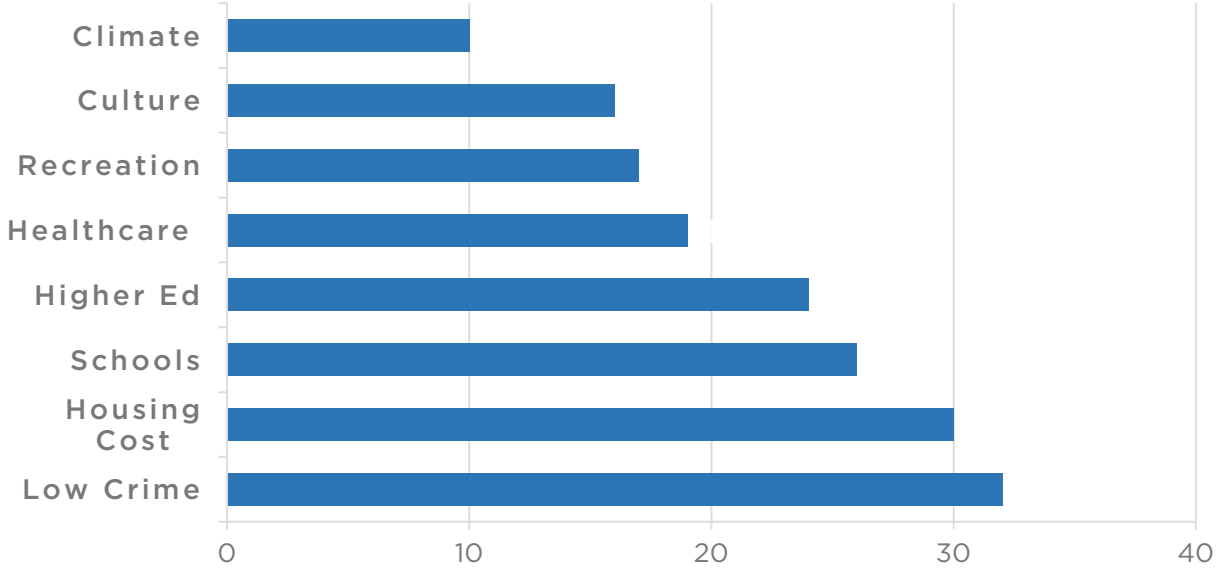
WHAT IS THE MOST IMPORTANT ROLE OF GOVERNMENT IN BUSINESS DEVELOPMENT?



WHAT ELEMENTS ARE MOST IMPORTANT TO YOU IN A BUSINESS ENVIRONMENT?



WHAT ELEMENTS ARE MOST IMPORTANT TO YOU FROM A QUALITY OF LIFE PERSPECTIVE?



Annex C: Indiana Economic Development Cybersecurity Town Hall Series

The Indiana Economic Development Corporation hosted a series of engagements across the State of Indiana known as the "Cybersecurity Town Hall Series." In total, 7 cybersecurity town halls were conducted across the state (Bloomington, Columbus, Evansville, Fort Wayne, Portage, Westgate, and West Lafayette). The stated objectives for these events were:

- To define the cybersecurity market in Indiana through direct engagement with cybersecurity providers and consumers.
- To identify economic development/business development opportunities within cybersecurity/information security.
- To educate cybersecurity providers and consumers about state incentives and programs available through the IEDC, Indiana Procurement Technical Assistance Center, and to Indiana Small Business Development Center.

Additional goals included identifying business to business opportunities for participants, general networking, and conducting an Indiana asset inventory.

Participants included cybersecurity solution providers who provide Identity and Access Management (IAM), risk and compliance management, encryption, Data Loss Prevention (DLP), Unified Threat Management (UTM), firewall, antivirus/antimalware, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), security and vulnerability management, disaster recovery, Distributed Denial of Service (DDoS) mitigation, web filtering, and other services.

Other participants were cybersecurity service providers specializing in managed services, professional services including consulting, training and education, support and maintenance, design and integration, and risk and threat assessment. Cybersecurity consumers across the following verticals also participated: aerospace and defense, government and public utilities, Banking, Financial Services, and Insurance (BFSI), IT and telecom, healthcare, retail, and manufacturing. Higher education and the military also participated.

Locations	Key Discoveries
Bloomington	• Opportunities to unlock intellectual property from higher education. • An innovation and entrepreneur community that could benefit from economic gardening. • Many assets and individuals that could be more effectively engaged by the state.
Columbus	• A high concentration of cybersecurity expertise and need surrounding advance manufacturing and industrial control systems. • A need for local cybersecurity certification training. • A desire to leverage military assets. • A Shortage of workforce. • A need for small and mid-size business cybersecurity solutions.
Evansville	• A desire for better communication within the state on cybersecurity information and initiatives. • A high concentration of expertise within utilities (energy). • A high concentration of cybersecurity expertise and need surrounding advance manufacturing and industrial control systems. • A need for small and mid-size business cybersecurity solutions. • A shortage of workforce.
Fort Wayne	• A need and desire to develop regional cybersecurity strategies. • A high concentration of expertise in health care, medical devices and advanced manufacturing. • A need for small and mid-size business cybersecurity solutions. • A shortage of workforce.

Portage	• A need for small and mid-size business cybersecurity solutions. • A need and desire to develop regional cybersecurity strategies. • A desire to leverage military assets. • A shortage of workforce.
Westgate	• A desire to leverage military assets. • Many assets and individuals that could be more effectively engaged by the State. • A need for investment in infrastructure. • A shortage of workforce.
West Lafayette	• Many assets and individuals that could be more effectively engaged by the State. • Opportunities to unlock intellectual property from higher education. • An innovation and entrepreneur community that could benefit from economic gardening.

Annex D: Indiana Cybersecurity Engagement Activities

Date	Category	Event	Representative	Location
June 24, 2016	State	Infragard Food and Agriculture Sector Event	Advisor for Cybersecurity	Atlanta, IN
June 26-27, 2016	International	Israel Cybersecurity Delegation	Governor, Secretary of Commerce, Chief Innovation Officer, Advisor for Cybersecurity	Indianapolis, IN
June 30, 2016	State	CXO Conference	Advisor for Cybersecurity	Indianapolis, IN
July 14, 2016	State	Innovation Showcase	Advisor for Cybersecurity	Indianapolis, IN
July 26-27, 2016	National	CSWC Microelectronics Integrity Symposium	Chief Innovation Officer, Advisor for Cybersecurity	Indianapolis, IN
August 2-5, 2016	National	Black Hat	Advisor for Cybersecurity	Las Vegas, NV
August 22, 2016	State	Association for Financial Professionals of Indiana	Advisor for Cybersecurity	Indianapolis, IN
September 1, 2016	State	Indy Big Data Conference	Chief Innovation Officer, Advisor for Cybersecurity	Indianapolis, IN
September 11-15, 2016	National	Infragard National Summit	Advisor for Cybersecurity	Orlando, FL
September 29, 2016	State	Center for Applied Cybersecurity Research Summit	Advisor for Cybersecurity	Indianapolis, IN
October 13, 2016	State	Centric Day of Innovation	Advisor for Cybersecurity	Indianapolis, In
October 24-27, 2016	National	ICS Cybersecurity Conference	Advisor for Cybersecurity	Atlanta, GA
November 22, 2016	State	Indiana Cybersecurity State of the State	Advisor for Cybersecurity	Indianapolis, IN
January 18, 2017	National	Atlanta A-List	Advisory for Cybersecurity	Indianapolis, IN
January 29 – February 3, 2017	International	CyberTech	Secretary of Commerce, Chief Innovation Officer, Advisor for Cybersecurity, Director of Field Operations	Tel Aviv, Israel
February 13-17, 2017	National	RSA	Advisor for Cybersecurity	San Francisco, CA
March 7-9, 2017	International	International Resiliency Conference	Advisor for Cybersecurity	New Orleans, LA
March 30 - April 1, 2017	National	Women in Cybersecurity	Advisor for Cybersecurity	Tucson, AZ
April 17-19, 2017	State	Center for Education and Research in Information Assurance and Security Symposium	Chief Innovation Officer, Advisor for Cybersecurity	West Lafayette, IN
April 21, 2017	State	Indiana Aerospace and Defense Council Breakfast	Governor, Secretary of Commerce, Chief Innovation Officer, Advisor for Cybersecurity	Indianapolis, IN

APPENDIX D.4
ELECTIONS COMMITTEE

ELECTION COMMITTEE STRATEGIC PLAN

Chair: Secretary Connie Lawson | Co-Chair: Beth Dlug

September 2018
Indiana Executive Council on Cybersecurity

Election Committee Plan

Contents

Committee Members **6**
Introduction **8**
Executive Summary **10**
Research **13**
Deliverable: Statewide Voter Registration System (SVRS) Cybersecurity Enhancements **20**
General Information 20
Implementation Plan 21
Evaluation Methodology 24
Deliverable: SVRS Network User Access Control Enhancement **26**
General Information 26
Implementation Plan 27
Evaluation Methodology 31
Deliverable: Election System Physical and Logical Security Controls **34**
General Information 34
Implementation Plan 35
Evaluation Methodology 38
Deliverable: Post-Election Risk Limiting Audit Standards and Pilot Program **40**
General Information 40
Implementation Plan 41
Evaluation Methodology 46
Deliverable: Cyber Threat Awareness and Training for County Election Administrators **48**
General Information 48
Implementation Plan 49
Evaluation Methodology 52
Deliverable: Election Day Cybersecurity Tabletop Exercises **55**
General Information 55
Implementation Plan 56
Evaluation Methodology 59
Deliverable: Indiana Best Practices Manual for the Operation of Election Equipment **61**
General Information 61
Implementation Plan 62

Evaluation Methodology 66
Deliverable: Election Day Cybersecurity Emergency Preparedness Plans 68
General Information 68
Implementation Plan 69
Evaluation Methodology 72
Deliverable: Election Day Cybersecurity Monitoring and Rapid Response Technical Support 74
General Information 74
Implementation Plan 75
Evaluation Methodology 78
Deliverable: Election Cybersecurity Public Education and Awareness 80
General Information 80
Implementation Plan 81
Evaluation Methodology 84
Deliverable: Election Cybersecurity Incident Response and Communications 86
General Information 86
Implementation Plan 87
Evaluation Methodology 90
Deliverable: Catalog and Summaries of Best Election Cybersecurity Reports and Guides 92
General Information 92
Implementation Plan 93
Evaluation Methodology 96
Supporting Documentation 98
Center for Internet Security (CIS) Handbook for Elections Infrastructure Security 99
Department of Homeland Seucirty (DHS) Multi-State Information Sharing and Analysis Center (MS-ISAC) ISAC Pilot for Eelction Infrastructure 174
Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) Common Cyber Security Language 193
Election Assistance Commission (EAC) Glossary of Common Cybersecurity Terms 201
Election Assistance Commission (EAC) U.S. Election Systems as Critical Infrastructure Addendum I: Glossary of Key Terms and Acronyms 209
Harvard Kennedy School Belfer Center Campaign Cybersecurity Playbook 222
Harvard Kennedy School Belfer Center Election Cyber Incident Communications Coordination Guide 249

Harvard Kennedy School Belfer Center The State and Local Election Cybersecurity Playbook 284

National Association of Elections Officials Election Center Elections Cybersecurity Checklist 357

Voting System Technical Oversight Program at Ball State University (VSTOP) Indiana Best Practices Manual for the Operation of Election Equipment 366

Voting System Technical Oversight Program at Ball State University (VSTOP) Risk Limiting Audit (RLA) Pilot 395

Voting System Technical Oversight Program at Ball State University (VSTOP) Risk Limiting Audit (RLA) Pilot Report 454

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Connie Lawson	Secretary of State	Secretary of State	Chair	Voting
Beth Dlug	Allen County	Elections Director	Co-chair	Advisory
Seth Cooper	Baker Tilly	Project Manager	Full Time	Advisory
Brad King	Indiana Election Division	Co-Director	Full Time	Advisory
Angie Nussmeyer	Indiana Election Division	Co-Director	Full Time	Advisory
Laura Herzog	Hendricks County	Elections Supervisor	Full Time	Advisory
Jay Phelps	Bartholomew County	Clerk	Full Time	Advisory
Jay Bagga	Ball State University	Co-Director, VSTOP	Full Time	Advisory
Sean Fahey	GCR	Elections and Campaign Finance Director	Full Time	Advisory
Dave Sturgeon*	Tippecanoe County	CIO	Full Time	Advisory
Brandon Clifton	Secretary of State	Deputy Secretary of State	As Needed	Advisory
Valerie Warycha	Secretary of State	Director of Communications	As Needed	Advisory
Jerry Bonnet	Secretary of State	General Counsel	As Needed	Advisory
Thomas Vessely	Secretary of State	Director of IT	As Needed	Advisory
Patrick Glover	Secretary of State	Asst. Director of IT	As Needed	Advisory
Gerry Baliey	iLab LLC	Director	As-Needed	Advisory

*Resignation effective 6/30/2018

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Interaction with several leading election cybersecurity organizations and initiatives.
  - Intelligence and situational awareness - evaluation of information, experiences, perspectives and concerns from across the sector.
  - Identification and assessment of cybersecurity vulnerabilities - i.e. phishing exercises, cyber hygiene assessments, and election system physical security and logical security controls.[1]
  - Identification and assessment of election cybersecurity authoritative information and best practices.

- **Research Findings**
  - Major election systems (voting systems, electronic poll books and associated equipment, software, and documentation) cybersecurity concerns center on Statewide Voter Registration Systems (SVRS), voting equipment physical and logical security controls, and network security.
  - Election cybersecurity involves systems and processes in use before, during, and after Election Day, including:
    - network user training and access authentication
    - physical security and cybersecurity of election systems
    - training for election officials, administrators and poll workers
    - network monitoring
    - election system certification and testing
    - election system physical and logical security controls
    - voting, tabulation, results reporting, post-election risk limiting audits
    - incident response and public communications
  - Election cybersecurity also encompasses networking with national and state security agencies and sector coordinating councils, training, incident response planning, and public awareness.

- **Committee Deliverables**
  - Statewide Voter Registration System (SVRS) Cybersecurity Enhancement
  - SVRS Network User Access Control Enhancement
  - Election System Physical and Logical Security Controls Assessments and Guides
  - Post-Election Risk Limiting Audit Standards and Pilot Program (included in the deliverable "Indiana Best Practices Manual for Operation of Election Equipment" below).
  - Cyber Threat Awareness and Training for County Election Administrators
  - Election Day Cybersecurity Tabletop Exercises
  - Indiana Best Practices Manual for the Operation of Election Equipment
  - Election Day Cybersecurity Emergency Preparedness Plans
  - Election Day Cybersecurity Monitoring and Rapid Response Technical Support

[1]Logical Security consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network. It is a subset of computer security.

- Election Cybersecurity Public Education and Awareness
- Election Cybersecurity Incident Response and Communications.
- Catalog and Summaries of Best Election Cybersecurity Reports and Guides.

• **Additional Notes & References**

- Notwithstanding heightened concerns resulting from the discovery of foreign attempts to penetrate voter registration systems prior to the 2016 General Election, election security and cybersecurity are not new issues in the realm of election administration. As of mid-2018 the election cybersecurity environment remains dynamic and of continuing public concern.
- The Secretary of State and Indiana Election Division have been, and continue to work, closely with U.S. Department of Homeland Security (USDHS), the Election Infrastructure Multi-State Information Sharing Analysis Center (MS-ISAC), the National Association of Secretaries of State (NASS) Election Cybersecurity Task Force, the Indiana Department of Homeland Security (IDHS) and Indiana National Guard (INNG), the Voting System Technical Oversight Program at Ball State University (VSTOP) and other government, academic, and industry resources.

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Well before the 2016 Election cycle, which gave rise to the national push for election cybersecurity. Indiana was aware and preparing to respond to the threat. In 2014 and 2015, the Secretary of State and the Indiana Election Division identified the need for Statewide Voter Registration System (SVRS) modernization and IT security enhancements. In furtherance of those priorities, Indiana developed a modernization roadmap and budget proposal, which was authorized and fully funded by the Indiana General Assembly in 2017.
    b. Training on security concepts for county IT support; information from vendors regarding best practices; phishing exercises for county election staff; continual training and awareness for county election officials, administrators and poll workers.
    c. Received and responded to national security agencies, industry, and association intelligence gathering and situational awareness. Participated in national and state forums for information gathering, exchange, analysis, and response coordination.
    d. Engaged cybersecurity assessment programs provided by USDHS and commercial vendors.
    e. Electronic poll book vendors have been surveyed regarding cybersecurity best practices. The survey included questions regarding server set up, security processes for election activity (including third-party servers on the cloud), backup and fail-safe data recovery procedures, file naming and versioning procedures and existence/maintenance of a security breach emergency crisis plan in the event there is unauthorized access to data and/or equipment. The results of this survey have been used to compile a list of best practices for cybersecurity of electronic poll books. Note: a similar survey is planned for election system vendors.
    f. VSTOP prepared the *Indiana Best Practices Manual for the Operation of Election Equipment.* The manual includes best practices for cybersecurity. Copies of the manual have been distributed to Election Officials in all 92 counties in Indiana.
    g. VSTOP organized the first post-election risk limiting audit (RLA) in Marion County which was also the first audit anywhere which used the Bayesian RLA method. Report submitted to the Indiana Secretary of State in August 2018.
    h. VSTOP has developed and recently launched an advanced professional election administrator certificate program, including specific cybersecurity training. The program's first class began in August 2018. The Secretary of State's office has provided scholarships for the first 16 students enrolled in the program.
    i. Election system and electronic poll book vendors with equipment used in Indiana elections are required to monitor and record performance anomalies. Performance anomalies are required to be reported to VSTOP for investigation and analysis as warranted and reported to the Secretary of State and Indiana Election Division.
    j. Legislation directed at election system physical security was enacted and implementation has begun.
    k. The Secretary of State and Election Division have initiated pre-election and Election Day emergency preparations and planning, including cyber events and coordination with national, state and local security and emergency response agencies.

l. The Secretary of State and National Association of Secretaries of State lobbied Congress for expedited approval of $380 million previously authorized, but un-released, Help America Vote Act funds approved in March 2018 for election security. Indiana applied for and received approval for approximately $7.6 million funding, approved in July 2018, and initiated planning for county sub-grants, SVRS upgrades, and cybersecurity initiatives. As a result of the State's proactive election cybersecurity initiatives, Indiana expects to have met its 5% federal grant match obligation.
m. VSTOP was among the founding institutions of the annual State Certification Testing of Voting Systems National Conference. The academic conference established in 2011 focuses on election security (http://bowencenterforpublicaffairs.org/institutes/policy-research/election-admin/conference). This conference was held in Indianapolis in 2012.
n. The Secretary of State and Election Division will be participating in an election cybersecurity session at the upcoming Cybertech Midwest Conference (October 2018, Indianapolis, Indiana).

2. What (or who) are the most significant cyber vulnerabilities in your area?

a. Malicious cyber hacking and unauthorized access to voter registration system data; particularly initiated by a sophisticated domestic or overseas perpetrator.
b. Cyberattacks aimed at: political parties, campaigns and candidates; the voter registration database system and user network; electronic poll books; election systems; and election result reporting systems managed by state and county election officials.
c. Malicious, anonymous, false or misleading social media activity aimed at political parties, campaigns and candidates.
d. Identifying cyberattacks or other election interference.
e. The voting systems physical security (addressed by SEA 327-2018), and election system logical security (addressed by certification standards, testing, monitoring and post-election risk-limiting audits).
f. Lack of network user and public awareness of cybersecurity principles and threats (addressed by communications, training, and uniform adherence to security protocols and best practices).
g. Any unaddressed actual or perceived cyber threat that adversely affects voter confidence.

3. What is your area's greatest cybersecurity need and/or gap?

a. Sophisticated cyber threat intelligence gathering, monitoring, and response as provided by national security agencies, sector coordinating councils and specialized vendors.
b. Identifying the presence of undesirable voting system cyber risk events and a process to assess the impact on counties, vendors and the State.
c. Identifying, verifying and implementing best cybersecurity practices for election systems, networks, election officials, administrators and poll workers.
d. Identifying, verifying and implementing best practices for election system physical and logical security.

e. Control or mitigation of false or misleading social media activity aimed at election interference.
f. Development of coordinated cyber incident communications and response.
g. Public awareness and communications.

4. What federal, state, or local cyber regulations is your area beholden to currently?

a. Federal and State election laws and administrative regulations (i.e. National Voting Rights Act, National Voter Registration Act, Help America Vote Act, Indiana Election Code).
b. Election system certification rules and protocols promulgated and administered by the Indiana Election Commission and Election Assistance Commission.
c. Indiana testing and certification requirements for election systems and electronic poll books.
d. Indiana Office of Technology cybersecurity standards and requirements for state agencies.
e. County policies and resolutions including cybersecurity protocols adopted by County Election Boards.

5. What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?

a. Handbook for Elections Infrastructure Security – Center for Internet Security.
b. The State and Local Election Cybersecurity Playbook - Harvard Kennedy School Belfer Center.
c. Campaign Cybersecurity Playbook - Harvard Kennedy School Belfer Center.
d. Election Cyber Incident Communications Coordination Guide – Harvard Belfer Center.
e. Elections Security Checklist - National Association of Elections Officials Election Center.
f. SEA 327-2018 Voting System Security – Indiana Election Division Presentation.
g. Indiana Best Practices Manual for the Operation of Election Equipment - Voting System Technical Oversight Program at Ball State University.
h. Post-Election Risk Limiting Audit Pilot, Marion County Indiana, May 2018 - Voting System Technical Oversight Program at Ball State University.
i. Risk Limiting Audit (RLA) Pilot Conducted In Marion County, Indiana in May 2018; report submitted to the Indiana Secretary of State in August 2018 – Voting System Technical Oversight Program at Ball State University.
j. US Elections System as Critical Infrastructure – Addendum I: Glossary of Key Terms and Acronyms - U.S. Election Assistance Commission.
k. NASS Election Cybersecurity Task Force Survey – National Association of Secretaries of State.
l. ISAC Pilot for Election Infrastructure – DHS/EI-ISAC.
m. Glossary of Common Cybersecurity Terms – U.S. Election Assistance Commission.
n. Common Cyber Security Language – U.S. DHS National Cybersecurity and Communications Integration Center (NCCIC).
o. National Conference of State Legislatures Election Security: State Policies: http://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. Handbook for Elections Infrastructure Security – Center for Internet Security.
    b. The State and Local Election Cybersecurity Playbook - Harvard Kennedy School Belfer Center.
    c. Campaign Cybersecurity Playbook - Harvard Kennedy School Belfer Center.
    d. Election Cyber Incident Communications Coordination Guide – Harvard Belfer Center.
    e. Elections Security Checklist - National Association of Elections Officials Election Center.
    f. SEA 327-2018 Voting System Security – Indiana Election Division Presentation.
    g. Indiana Best Practices Manual for the Operation of Election Equipment - Voting System Technical Oversight Program at Ball State University.
    h. Risk Limiting Audit (RLA) Pilot Conducted In Marion County, Indiana in May 2018; report submitted to the Indiana Secretary of State in August 2018 – Voting System Technical Oversight Program at Ball State University.
    i. US Elections System as Critical Infrastructure – Addendum I: Glossary of Key Terms and Acronyms - U.S. Election Assistance Commission.
    j. NASS Election Cybersecurity Task Force Survey – National Association of Secretaries of State.
    k. ISAC Pilot for Election Infrastructure – DHS/EI-ISAC.
    l. Glossary of Common Cybersecurity Terms – U.S. Election Assistance Commission.
    m. Common Cyber Security Language – U.S. DHS National Cybersecurity and Communications Integration Center (NCCIC).

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. The National Association of Election Officials Election Center has promulgated and distributed an Elections Security Checklist.
    b. The Harvard Belfer Center and USDHS have developed and are presenting Election Tabletop Exercises to election officials and administrators.
    c. The National Association of Secretaries of State Election Cybersecurity Task Force surveyed states on election cybersecurity practices.
    d. The US Election Assistance Commission has posted materials, documents and videos, related to elections cybersecurity.
    e. The National Conference of State Legislators and California have created cybersecurity task forces.
    f. The National Association of Secretaries of State is tracking federal election security initiatives and the National Council of State Legislators is tracking state election security legislation.
    g. The annual State Certification Testing of Voting Systems National Conference focuses on elections security. (see: http://bowencenterforpublicaffairs.org/institutes/policy-research/election-admin/conference/raleigh-conference-2018/%20raleigh-conference-2018-agenda)
    h. Colorado and Wisconsin have developed extensive cybersecurity training programs for local election administrators.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Year One – priority programs developed; Year Three- deliverables developed with training programs; Year Five – no successful penetration of election systems or databases essential to conducting elections.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. Indiana's county election officials and administrators need cybersecurity communications training to promptly and accurately inform the public regarding the safety and security of the systems and to respond to cybersecurity incidents in an appropriate and coordinated fashion.
    b. A statewide public awareness campaign is being developed and will be launched in time for the November 2018 General Election.
    c. VSTOP has developed and launched an advanced professional election administrator certificate program. The program's first class began in August 2018. The Secretary of State's office has provided scholarships for the first 16 students enrolled in the program.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. In addition to the Secretary of State's office and Election Division, every Indiana county has election workforce including officials, administrators and poll workers. The IT and cybersecurity workforce within each county varies according to population, resources and other factors.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. A trained, ready workforce should attract cyber companies. Programs at Indiana's universities, colleges and technical schools providing state of the art training for the IT and cybersecurity workforce should be supported.
    b. Indiana can continue to host leading cybersecurity conferences such as the Cybertech Midwest Conference.
    c. State agencies can gather information regarding potential cybersecurity service vendors and issue a public request for proposals (RFP)/request for quotations (RFQ)/Quantity Purchase Agreement (QPAs) for cybersecurity assessments and initiatives after needs and priorities have been identified.

12. **What are your communication protocols in a cyber emergency?**
    a. Under Indiana law, a cyber incident that could impact election administration is to be immediately reported to the Secretary of State.
    b. The Secretary will communicate the details of the incident to appropriate responding security and intelligence agencies and Election Division.
    c. The Election Division will communicate with county election officials and administrators, state agencies, vendors, association and industry partners as appropriate.
    d. The Secretary of State will coordinate public communications through media channels as warranted.

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. Cybersecurity awareness training, communication, risk assessment and risk mediation for state agencies, employees and IT vendors.
b. Ongoing cybersecurity awareness training for all Hoosiers.

Deliverable: Statewide Voter Registration System (SVRS) Cybersecurity Enhancements

Deliverable: Statewide Voter Registration System (SVRS) Cybersecurity Enhancements

General Information

1. **What is the deliverable?**
    a. Enhanced Statewide Voter Registration System (SVRS) cybersecurity though installation and operation of additional critical protections to prevent and detect unauthorized intrusion.

2. **What is the status of this deliverable?**
    a. 100% complete

3. **Which of the following IECC goals does this deliverable meet?**

☐ Establish an effective governing structure and strategic direction.
☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
☐ Strengthen best practices to protect information technology infrastructure.
☐ Build and maintain robust statewide cyber-incident response capabilities.
☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

☐ Research – Surveys, Datasets, Whitepapers, etc.
☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Secure the State's voter registration database system with state-of-the-art protections in coordination with agency partners.

6. **What metric or measurement will be used to define success?**
    a. Prevention of unauthorized access to SVRS.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. The State as custodian and administrator of the SVRS, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State resources were used to implement these enhancements.
    b. Some portion of Federal Help America Vote Act (HAVA) funds released to Indiana in 2018 may be allocated to maintenance of these enhancements.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Indiana Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Maintaining the highest level of security for the SVRS will be an ongoing and likely evolving effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Protocol Utilization	SOS Exec. Staff	100%	N/A	
Implement Critical Protections	SOS IT Staff	100%	N/A	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes – see below:

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1-2 hrs	N/A	Technical	State	HAVA	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Enabling critical protections to improve the security posture of our elections network.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Having these critical protections provides an additional layer of security making it less likely for any threat to successfully infiltrate the network.

19. What is the risk or cost of not completing this deliverable?

a. One less layer of security.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success can be measured by the data/metrics generated from these efforts.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Given this effort requires support from a third party vendor. Delays in anticipated completion and service disruptions are possible.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Certain protections will require maintenance.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Statewide Voter Registration System Core Team.

27. Can this deliverable be used by other sectors?

a. No – due to unique system functions and characteristics.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. County election officials and administrators are aware of the SVRS security enhancements.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes – to the extent required by the Indiana Open Door and Public Records Acts.

30. What are other public relations and/or marketing considerations to be noted?

a. None – SVRS security protocols and enhancements are not public facing.

Evaluation Methodology

Objective 1: Indiana Secretary of State Office will begin utilizing additional security protocols in 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Statewide Voter Registration System (SVRS) Network User Access Control Enhancement

Deliverable: SVRS Network User Access Control Enhancement

General Information

1. **What is the deliverable?**
    a. Statewide Voter Registration System (SVRS) network user access security upgrades.

2. **What is the status of this deliverable?**
    a. Indiana's first statewide voter registration system successfully began operating in all 92 counties in December 2005, making Indiana one of the states to achieve the 2006 implementation deadline for SVRS set by the federal HAVA law. During the two years before this rollout, the State worked with skilled system designers to ensure that SVRS included numerous safeguards to prevent the deliberate or accidental corruption of voter registration data. In the years following the 2005 rollout, Indiana continued to learn from both SVRS county system users and from the experience of other states to identify and implement additional enhancements to prevent intrusions into the system. The existing SVRS system has a robust framework to safeguard voter registration data.
    b. Even before heightened national awareness of cybersecurity issues during and after the 2016 election, Indiana had begun studying and implementing innovative features to further improve SVRS security. With the assistance of specialized vendors and project managers, technology and protocols for SVRS user access security upgrades were specified and successfully tested with strategically selected user groups. The user access upgrade pilot program is 100% complete. Implementation of multi-factor authentication have commenced. All users will utilize multi-factor authentication or token for the November 2018 General Election.

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Implementation of state-of-the-art user access controls including multi-factor authentication tools.

6. **What metric or measurement will be used to define success?**
    a. Implementation of security upgrades, metrics from ongoing monitoring.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State as custodian and administrator of the SVRS, system users, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State resources were used to implement these enhancements.
    b. Some portion of Federal Help America Vote Act (HAVA) funds released to Indiana in 2018 may be allocated to maintenance of these enhancements.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Indiana Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Multi-Factor Authentication	SOS Office and Indiana Election Division	100%	December 2017	
Multi-Factor Authentication	SOS Office and Indiana Election Division	100%	December 2017	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Multi-Factor Authentication.	The physical token is required for participating pilot counties to access SVRS.	$100,000.	N/A	State	HAVA	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. New authentication features were added to the Statewide Voter Registration System (SVRS) to increase the security of the system.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Counties participating in the pilot will reduce their cybersecurity risk since multi-factor authentication expands the validation protocol.
b. Because most attacks are targeted during after-hours (in an effort to prevent detection), an additional validation tactic will be required for users attempting to access SVRS during those after-hours.

19. What is the risk or cost of not completing this deliverable?

a. Not completing these deliverables inscreases risk that an attacker might gain access to SVRS. It is a method of confirming a user's claimed identity by utilizing a combination of multiple factors of authentication.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. A key success objective includes reducing cybersecurity threats and maintaining needed functionality in SVRS. User Acceptance Testing (UAT) validates that the software functionality meets the requirements in real-world scenarios and is a key systematic metric used to measure success. Users are able to provide enhancement suggestions at any time, which help evolve the functionality on an ongoing basis. Specific to the pilot, every six weeks' feedback is collected and evaluated from participating county users to identify and resolve issues, and will be used to evaluate the pilot success for consideration of a statewide rollout.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes.
b. Many states are inquiring about similar projects used in Indiana. New Jersey, Colorado, and West Virginia are believed to have similar projects completed or in-progress.

22. Are there comparable jurisdictions (e.g. other states) that do not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes.
b. Arizona did not use a comparable project in the 2016 General Election, and a county user experienced an intrusion.Arizona did not use a comparable project in the 2016 General Election, and a county user experienced an intrusion.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. This is not applicable since deliverables were completed within the agreed upon timeline and budget.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this effort if it requires ongoing sustainability?

a. The Indiana Secretary of State, Indiana Election Division, 92 county election officials, and vendor partners will continue to evaluate best practices and, as situations warrant, enhance security capabilities as needed. The Indiana Elections Cybersecurity Council does not need to set aside resources for assistance.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. All 92 county election officials are aware of the implementation of these deliverables.

27. Can this deliverable be used by other sectors?

a. Yes.
b. All other sectors looking to implement multi-factor authentication needed for user access to sensitive or private data.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. The Indiana Secretary of State, Indiana Election Division, and all 92 SVRS users.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes – to the extent required by the Indiana Open Door and Public Records Acts.

30. What are other public relations and/or marketing considerations to be noted?

a. Development of messaging for the public without divulging any confidential information, which could compromise security.

Evaluation Methodology

Objective 1: SOS Office and Indiana Election Division will implement the Statewide Voter Registration System (SVRS) user access/authentication upgrades with one-hundred percent of counties by January 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Objective 2: SOS Office and Indiana Election Division will launch a Two-Factor Authentication Token Pilot by March 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 3: SOS Office and Indiana Election Division will provide a report on Two-Factor Authentication Token Pilot by May 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Election System Physical and Logical Security Controls

Deliverable: Election System Physical and Logical Security Controls

General Information

1. **What is the deliverable?**
   a. Best practices for voting system logical and physical security. This deliverable is included in the deliverable "Indiana Best Practices Manual for Operation of Election Equipment."

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Best practices guidelines for protecting, testing and storing voting systems.

6. **What metric or measurement will be used to define success?**
   a. Availability and acceptance and use of guidelines. Incorporation of guidelines into statutory requirements.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
   a. State and County election officials and administrators, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. The Indiana Voting System Technical Oversight Program at Ball State University (VSTOP).

12. **Who should be main lead of this deliverable?**
    a. The Indiana Voting System Technical Oversight Program at Ball State University (VSTOP).

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Education on the Physical and Cyber Security Requirements in Election Codes	VSTOP	100%	July 2018	This is also tied to deliverable no. 7, which includes a best practices manual on the operation of election equipment
New Security Features in SEA 327/Public Law 100 (2018)	VSTOP	100%	July 2018	
Continued Encouragement of Legislation that Promotes Physical and Cyber Security of Elections	VSTOP		On-going	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Increased education and awareness of physical and cybersecurity best practices among election officials at the county and State level.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This will help train election officials to efficiently manage security risks. The estimated costs are unknown, for instance Public Law 100 (2018) allows counties to request funding assistance for certain security measures.

19. What is the risk or cost of not completing this deliverable?

a. Election process will be more vulnerable to physical and cybersecurity risks.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. That the County Election Officials are able to successfully implement the requirements of the law and the best practices as specified in the deliverable.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes.
b. VSTOP will supplement after consultation with Election Assistance Commission (EAC)

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No. VSTOP will supplement after consultation with EAC. VSTOP will supplement after consultation with EAC.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None at this time

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Experience gained from implementing this deliverable could lead to recommendations of further revisions or additions to the Indiana Election Code.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. VSTOP has consulted various sources, such as the websites of the EAC, Election Center, National Conference of State Legislatures (NCSL) and Belfer Center at Harvard University.

27. Can this deliverable be used by other sectors?

a. No.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Secretary of State Office, Indiana Election Division (as well as Indiana Election Commission) and Indiana County Clerks and Election Officials.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. It may be beneficial for the public to know that Indiana takes great care and trains Election Officials in the best practices in physical and cybersecurity. In addition, publicity regarding the best practices being followed, as well as required, also provides assurance to voters and jurisdictions holding elections.

Evaluation Methodology

Objective 1: Indiana Voting System Technical Oversight Program will develop and distribute the Best Practices for Voting System Logical and Physical Security Manual to all Indiana counties in 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Post-Election Risk Limiting Audit Standards and Pilot Program

Deliverable: Post-Election Risk Limiting Audit Standards and Pilot Program

General Information

1. **What is the deliverable?**
   a. Post-election risk limiting audit standards and pilot program.

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Availability and implementation of a validated post-election risk limiting audit procedure.

6. **What metric or measurement will be used to define success?**
   a. Statistical confidence measures as well as general public confidence in election outcomes.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State and county election officials and administrators, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. The US Election Assistance Commission (EAC) provided expertise and assisted in the completion of this deliverable.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. The US Election Assistance Commission (EAC).

12. **Who should be main lead of this deliverable?**
    a. The Voting System Technical Oversight Program at Ball State University.

13. **What are the expected challenges to completing this deliverable?**
    a. Availability of pilot counties in Indiana where this deliverable can be tested.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort depending on determination of pilot RLA.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Research and Planning of RLA	VSTOP	100%	May 2018	Election Assistance Commission (EAC) is also assisting
Pilot RLA in Marion County	VSTOP	100%	June 2018	Pilot conducted May 2018.
Presentation on RLA Pilot at National State Certification Conference in Raleigh, NC	VSTOP	100%	June 2018	SOS approval received.
Post-Audit Analysis	VSTOP, Marion County & EAC (Jerome Lovato)	100%	August 2018	Report prepared.
Observation of Denver County RLA for Primary 2018	VSTOP Team Member	100%	August 2018	Report in preparation.
Pilot in Three Michigan Counties December 2018	Michigan	10%	January 2019	Draft Pilot Proposal/Plan in Progress; VSTOP is assisting the State of Michigan.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No.
b. At this time for the Pilot RLA's, VSTOP Team members, County Election Officials, and EAC will contribute their time. If RLA's are adopted and instituted in Indiana in all counties, using an optical scan voting system as its primary voting system, funding for an FTE or ½ FTE and/or resources may be required.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Post-election audits are gaining increasing acceptance across the country and are required by law in some states. Performing RLA results in increased confidence in election results.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. If Risk Limiting Audits are deemed successful and used in the future it could increase assurances in the election tallying process, which could then lessen the number of recounts and election contests that occur in counties using optical scan voting systems as its primary voting system.

19. What is the risk or cost of not completing this deliverable?

a. If Indiana does not move forward in election security best practices, this can lead to a decrease in voter confidence in election results.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The timely completion of an RLA for one county-wide race in the 2016 General and 2018 Primary Marion County elections. Ideally, we would like to complete three different audit methods: Comparison, Ballot-Polling, and the Bayesian Audit.
b. Increased statistical confidence measures.
c. Increased overall public confidence in elections and certain types of voting systems.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes.
b. Arapahoe County, Colorado instituted a pilot RLA in one County prior to instituting it in all counties, that we can use for comparison. In 2014, Cuyahoga County, Ohio, conducted a risk limiting audit for its gubernatorial race. Others may be added after consultation with EAC.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes.
b. Although many states, such as Colorado, Rhode Island, and Virginia require RLAs, most states do not.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The 2018 Primary absentee voting and preparations for Election Day resulted in the County staff, as well as the VSTOP and EAC team, assisting with the audit not being available until mid-May for the pilot.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes.
b. Currently, RLAs are not required in Indiana. If the pilot is deemed successful, Indiana may want to pursue legislation mandating their requirement in counties using optical scan voting systems as its primary voting system. Fiscal impact could include new costs, such as training, personnel and software.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. If RLAs were implemented in some or all of the 92 counties, then training, additional processes and forms, personnel, and potentially new software would be required.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. VSTOP has contacted Jerome Lovato Certification Program Specialist from the EAC, Dr. Ron Rivest of the Caltech/MIT Voting Technology Project, the Indiana Election Division Co-Directors, as well as the Marion County Election Director and Deputy Director.

27. Can this deliverable be used by other sectors?

a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Secretary of State Office, Indiana Election Division (as well as Indiana Election Commission) and Indiana County Clerks and Election Officials. See Supporting Documentation: Risk Limiting Audit (RLA) Pilot Conducted In Marion County, Indiana in May 2018; Report to the Indiana Secretary of State in August 2018 – Voting System Technical Oversight Program at Ball State University.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. It may be beneficial for the public to know that risk limiting audits are being looked into in the State since many other jurisdictions outside of Indiana are conducting them already. In addition, publicity regarding the successful completion of RLA can provide additional assurance to voters in counties using optical scan voting systems as its primary voting system that the results of an election are accurate.

Evaluation Methodology

Objective 1: Indiana Voting System Technical Oversight Program (VSTOP) will develop and implement an RLA pilot in Marion County by July 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indiana Voting System Technical Oversight Program (VSTOP) will provide a report by August 2018 on the July 2018 RLA pilot in Marion County.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Threat Awareness and Training for County Election Administrators

Deliverable: Cyber Threat Awareness and Training for County Election Administrators

General Information

1. **What is the deliverable?**
   a. Election cyber threat exercises and training for county election units (e.g. phishing exercises).

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Increased situational awareness of the cyber threat environment and implementation of cybersecurity best practices at the election county unit level.

6. **What metric or measurement will be used to define success?**
   a. Metrics from phishing exercises, surveys, and other assessments.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State and County election officials and administrators, and the general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State, Election Division and County Election Officials.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Create initial phishing exercise	SOS IT Staff	100%		
Deliver on-going training & awareness	SOS IT Staff	Ongoing		Content has been queued and will be delivered beginning April 2018

Resources and Budget

15. **Will staff be required to complete this deliverable?**
    a. No.

16. **What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)**
    a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Continued education and awareness to the staff of potential threats to physical and logical security.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. It will raise awareness and staff will be more vigilant with data sharing practices. No associated costs.

19. What is the risk or cost of not completing this deliverable?

a. The risk is having staff unaware or uninformed, creating the potential for data leaks.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The baseline has been set with the initial phishing campaign. Success will be measured by increased participation in training programs and decreased response to phishing attempts.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. None.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Ongoing coordination with counties to effectively conduct phishing campaigns.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Secretary of State and Indiana Election Division.

27. Can this deliverable be used by other sectors?

a. No.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Secretary of State and Indiana Election Division.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No.

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Indiana Secretary of State will implement and deliver a multi-year cybersecurity public awareness plan beginning in 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Eighty percent of Indiana election officials participate in state-offered training by November 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Objective 3: See a thirty-percent decrease in click-through rates of Indiana election officials in State phishing campaign by April 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Election Day Cybersecurity Tabletop Exercises

Deliverable: Election Day Cybersecurity Tabletop Exercises

General Information

1. **What is the deliverable?**
   a. Election security tabletop exercise program for state and local election officials and administrators.

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Develop and deliver a training exercise program for election officials and administrators.

6. **What metric or measurement will be used to define success?**
   a. Availability of the program for county election administrator use during the 2018 Election cycle.

7. **What year will the deliverable be completed?**
   a. 2018 and 2019.

8. **Who or what entities will benefit from the deliverable?**
   a. State and County election officials and administrators.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana National Guard may be utilized for a complete exercise in 2019.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Deliver tabletop exercises to counties on how to conduct elections	SOS Staff	25%	April 2019	

Resources and Budget

15. **Will staff be required to complete this deliverable?**
    a. Yes.

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0.5	0.25	Skilled	Agency	N/A	

16. **What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)**
    a. Election day equipment, exercise facilities.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The greatest benefit is providing consistent information to counties on conducting elections as well as awareness of potential threats or risks and methods for responding to them.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. The risk is reduced by increased training and execution of best practices.

19. What is the risk or cost of not completing this deliverable?

a. The risk is exposure of processes and information intended only for county election officials.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The baseline has yet to be established. The format for the tabletop exercises is being built off a model developed by the Belfer Center at Harvard.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Wisconsin.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability of county election administrators to participate (timeline constraint).

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Commitment to participation at the county level.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Secretary of State and Indiana Election Division.

27. Can this deliverable be used by other sectors?

a. No.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Secretary of State and Election Division.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No.

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Indiana Secretary of State will develop and deliver a training exercise program for election officials and administrators by October 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Secretary of State will conduct a tabletop election exercise by April 2019.
Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Indiana Best Practices Manual for the Operation of Election Equipment

Deliverable: Indiana Best Practices Manual for the Operation of Election Equipment

General Information

1. **What is the deliverable?**
   a. Best Practices Manual for the Operation of Election Equipment.

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Best practices Manual for Indiana election officials and administrators provides the most up-to-date considered best practices, promotes situational awareness and operational uniformity.

6. **What metric or measurement will be used to define success?**
   a. Completion and distribution of the manual for use in the 2018 General Election.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State and County election officials and administrators.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. U.S. Election Assistance Commission.

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Indiana Secretary of State Office (SOS) and Indiana Election Division (IED).

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Secretary of State Office (SOS) and Indiana Election Division (IED).

12. **Who should be main lead of this deliverable?**
    a. The Indiana Voting System Technical Oversight Program (VSTOP) at Ball State University.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Workshops on Material in the Manual at Southern & Northern District Clerk Conferences in Early March	VSTOP	100%	March 2018	
Research and Construction of the Manual	VSTOP	100%	March 2018	
Submit Draft to IED/SOS for approval and feedback	VSTOP	100%	June 2018	
Submit Draft to Counties for review and feedback	VSTOP	100%	June 2018	Sent to all 92 Counties in June 2018 and asked for comments.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Increased education and awareness of best practices for the operation of election equipment, including physical and cybersecurity of elections, among election officials at the county and State level.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This will help train election officials in efficient management of security risks.
b. At this time, we are not aware of any additional associated costs with production of a best practices manual that will not be absorbed through VSTOP's current budget. However, if the counties implement some of these best practices there may be new costs that are unknown at this time.

19. What is the risk or cost of not completing this deliverable?

a. Lack of knowledge regarding the best practices that are a part of Indiana Election Code, as well as some possible security risks not being properly managed.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion and distribution of a manual, as well as positive feedback and implementation of the best practices at the County level.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes. VSTOP consulted materials on the EAC website and Belfer Center resources.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. None known to VSTOP.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Ongoing monitoring and updating of evolving best practices.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. VSTOP has consulted various sources, such as the websites of the EAC, Election Center, National Conference of State Legislatures (NCSL) and Belfer Center at Harvard University.

27. Can this deliverable be used by other sectors?

a. No.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Secretary of State, Indiana Election Division (as well as Indiana Election Commission) and Indiana County Clerks and election administrators in all 92 counties.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. It may be beneficial for the public to know that Indiana takes great care and trains Election Officials in the best practices in physical and cybersecurity. In addition, publicity regarding the best practices being followed, as well as required, also provides assurance and confidence to voters and jurisdictions holding elections.

Evaluation Methodology

Objective 1: Indiana Voting System Technical Oversight Program (VSTOP) will develop the Indiana Best Practices Manual for the Operation of Election Equipment by July 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Election Day Cybersecurity Emergency Preparedness Plans

Deliverable: Election Day Cybersecurity Emergency Preparedness Plans

General Information

1. **What is the deliverable?**
    a. Election Day cyber incident and emergency preparedness plans for State and County election officials and administrators.

2. **What is the status of this deliverable?**
    a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Update existing Election Day emergency preparedness and response material to include cybersecurity for distribution prior to 2018 May Primary Election and future elections.

6. **What metric or measurement will be used to define success?**
    a. Completion and distribution of plans prior to the 2018 May Primary Election. Obtain feedback after the May election to update plans prior to the 2018 November General Election.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State and County election officials and administrators.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Government Service, Energy, Emergency Services, Pre to Post Incident, Local Government.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Plans for Indiana state and county election administrators	Secretary of State, Indiana Election Division	100%	April 2018	Working on cybersecurity incident updates.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes.

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
40	N/A	Admin.	Admin	Elections	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Up to date emergency preparedness plans for election officials, administrators and poll workers for the 2018 May Primary and November General Election.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Election officials, administrators and poll workers will have appropriate contacts for rapid assistance with emergency situations as well as procedural and legal guidelines for election disruptions.

19. What is the risk or cost of not completing this deliverable?

a. Risk of a significant or prolonged election disruption due to lack of preparation and delayed response. Delayed response increases the cost, time and complexity of correcting election interference. Disruptions and delays decrease public satisfaction and confidence in election outcomes.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. First, completing and distributing plans prior to the 2018 Primary Election. Second, usefulness of the plans in the event of an election disrupting emergency. Third, feedback from election officials, administrators and poll workers.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability of administrative resources, intervening emergencies, new contingencies, or changes in situational status.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Continually updating plans as needed, particularly prior to elections, as conditions and events warrant.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. The Indiana Election Division, emergency responders, and IT technical support resources.

27. Can this deliverable be used by other sectors?

a. Yes, but only to a degree. Generally, any government service provider could likely benefit from emergency and contingency plans. Election administration is a somewhat unique and specialized government service; therefore, the plans would need to be adapted to different sectors and activities.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. State and county election officials and administrators along with emergency responders.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No.

30. What are other public relations and/or marketing considerations to be noted?

a. The general public should be generally aware of the existence of emergency and contingency planning.

Evaluation Methodology

Objective 1: Indiana Secretary of State and Election Division will provide existing Election Day emergency preparedness and response material to include cybersecurity for distribution prior to May 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Election Day Cybersecurity Monitoring and Rapid Response Technical Support

Deliverable: Election Day Cybersecurity Monitoring and Rapid Response Technical Support

General Information

1. **What is the deliverable?**
   a. Election Day cybersecurity technical support program and resources.

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Cybersecurity technical support and resources (teams) to support State and local election officials and administrators.

6. **What metric or measurement will be used to define success?**
   a. Availability of adequate level of oriented and prepared cybersecurity technical support resources. Effective response to cybersecurity issues during 2018 May and November Elections.

7. **What year will the deliverable be completed?**

a. 2018

8. Who or what entities will benefit from the deliverable?

a. State and County election officials and administrators, and the general public.

9. Which state or federal resources or programs overlap with this deliverable?

a. U.S. and Indiana Departments of Homeland Security.

Additional Questions

10. What other committees and/or working groups will your team be working with to complete or plan this deliverable?

a. Government Service, Emergency Services, Pre/Post Incident, Local Government, Strategic Resource.

11. Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?

a. Secretary of State, Election Division, Indiana Office of Technology (IOT), Indiana Information Sharing and Analysis Center (IN-ISAC), DHS, IDHS, MS-ISAC, IECC, local units.

12. Who should be main lead of this deliverable?

a. Secretary of State and Election Division.

13. What are the expected challenges to completing this deliverable?

a. None.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Staff election IT/cybersecurity support call center on Election Day – with access to an assembly of technical resources for May Primary and November General Elections.	Secretary of State/Election Division	100%	April 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes (if Yes, please complete the following).

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
2-3	0	General IT	Agency	N/A	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Availability of an oriented, well connected emergency resource to assist, troubleshoot, and resolve Election Day IT or cybersecurity issues. Will help secure the election and assure the public.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. IT issues can be assessed and addressed quickly with real-time communications from cyber network monitoring sources. Cyber alerts can be quickly disseminated throughout the Election Day sector.

19. What is the risk or cost of not completing this deliverable?

a. Unaddressed IT or cybersecurity issues could hamper the elections and negatively impact public confidence.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Numbers of alerts, inquires, or issues.
b. Response capability.
c. Response time.
d. Response effectiveness.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The agency can't easily prepare and organize responsive resources for events not known or not likely to occur. Election administrators are expectedly quite occupied with regular responsibilities at this time.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. If the activity and resource can be made available (with modification as indicated) if it appears to have been helpful and useful this year.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Secretary of State and Election Division.

27. Can this deliverable be used by other sectors?

a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. County election officials and administrators.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No.

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Secretary of State will develop and implement an Election Day cybersecurity technical support program by April 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Secretary of State will develop an Election Day cybersecurity technical support program report and after action review with key partners by October 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Election Cybersecurity Public Education and Awareness

Deliverable: Election Cybersecurity Public Education and Awareness

General Information

1. **What is the deliverable?**
   a. Election security public education programming and coordination.

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☒ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Better informed public and news media. Capability for timely and accurate messaging.

6. **What metric or measurement will be used to define success?**
   a. Creation of content and communications plan. Assessment of public and news media knowledge and confidence in election security.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Elections sector, the general public, and the news media.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Communications, Public Awareness, Policy, Local Government.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Secretary of State.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Ongoing communications initiative to inform and reassure the public about government's awareness and management of the cyber threat environment.	Secretary of State	75%	October 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes.

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
2 - 3	1	Comm. Prof.	Agency	Fed. HAVA	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Maintaining public confidence in elections. Providing accurate information or responses to "fake or politicized news." General public understanding of the cyber threat environment.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This can improve/protect public perception of ongoing and existing cyber initiatives in place that are related to elections.

19. What is the risk or cost of not completing this deliverable?

a. Uncertain public confidence in state election administration.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success would be measured by the preparedness of content distribution and the quality of the information being released.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Allocation of agency fiscal and human resources.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Secretary of State and Indiana Election Division.

27. Can this deliverable be used by other sectors?

a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Combination of Technical, Communications and Executive leadership.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Secretary of State will develop a communications plan specific to election security by April 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Secretary of State will measure the success of communications plan efforts specific to election security by October 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Election Cybersecurity Incident Response and Communications

Deliverable: Election Cybersecurity Incident Response and Communications

General Information

1. **What is the deliverable?**
   a. Organize an election cybersecurity incident communications and response network.

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Capability to rapidly communicate a cyber incident or threat information across the election sector and allied cybersecurity interests, and coordinate response activities.

6. **What metric or measurement will be used to define success?**
   a. Identify participants. Obtain participant acknowledgements and protocol agreements.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. The election sector and general public.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Government Service, Energy, Communications, Public Awareness, Emergency Services, Cyber Sharing, Pre to Post Incident, and Local Government.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Secretary of State and Election Division, IDHS, DHS, State IOT and IN-ISAC, county and municipal units.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State and Election Division.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Establish and operate an Election Day cyber threat and incident response information and communications resource.	Secretary of State	100%	October 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1-2	0.25	General IT and Comm.	Agency	N/A	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Provide support to counties on identified issues and provide assurances to constituents that elections are well managed and secure.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable is intended to reduce the adverse impact to any identified/known issues. There are no direct costs associated with risk reduction.

19. What is the risk or cost of not completing this deliverable?

a. Unaddressed public concern that elections are not secure.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success will be defined in multiple parts: 1) the preparedness of the team in the event of an incident. 2) The quality of the resource as it relates to proper communications/support. 3) How effective the resource proves to be post-implementation.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Allocation of agency fiscal and human resources.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Secretary of State and Election Division.

27. Can this deliverable be used by other sectors?

a. No.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. County election officials and administrators.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Secretary of State will develop and distribute an Election Day cybersecurity incident communications and response to all Indiana election county officials by October 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Catalog and Summaries of Best Election Cybersecurity Reports and Guides

Deliverable: Catalog and Summaries of Best Election Cybersecurity Reports and Guides

General Information

1. **What is the deliverable?**
   a. Collection of relevant election security reports and guides, indexed, summarized and periodically updated. Place on a website for Indiana election sector use.

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☒ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Uniform library of relevant information and guides, indexed and summarized, for reference and use across the election sector.

6. **What metric or measurement will be used to define success?**
   a. Posting the materials, index and summaries on web page and notifying the election sector.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. State and County election officials and administrators.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None.

12. **Who should be main lead of this deliverable?**
    a. Secretary of State.

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Collection of materials with summaries	Secretary of State	75%	October 2018	

Resources and Budget

15. **Will staff be required to complete this deliverable?**
    a. No.

16. **What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)**
    a. None.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Uniform library of relevant information and guides, indexed and summarized, for State, county and local election officials and administrators to reference and use.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Effective situational awareness and familiarization with best practices and approaches. Increase uniformity of knowledge and practice across the sector.

19. What is the risk or cost of not completing this deliverable?

a. Risk is operating on outdated information as well as inefficiency due to duplication of time and resources spent surveying reports and literature.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Availability of summarized collection of relevant reports and articles at an easily accessible location. Reduce the number of relevant reports and guides from approximately 50 to the "top ten" reports and guides.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Few if any. Election officials, administrators and staff are periodically preoccupied with ongoing Elections (i.e. May Primary and November General Elections in 2018).

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Allocation of agency funds and human resources.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Secretary of State and Election Division.

27. Can this deliverable be used by other sectors?

a. No.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. State and county election officials and administrators, allied IT staff and vendors.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No.

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Secretary of State will develop an election cybersecurity library by October 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Center for Internet Security (CIS) Handbook for Elections Infrastructure Security
- Department of Homeland Security (DHS) Multi-State Information Sharing and Analysis Center (MS-ISAC) ISAC Pilot for Election Infrastructure
- Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) Common Cyber Security Language
- Election Assistance Commission (EAC) Glossary of Common Cybersecurity Terms
- Election Assistance Commission (EAC) U.S. Election Systems as Critical Infrastructure Addendum I: Glossary of Key Terms and Acronyms
- Harvard Kennedy School Belfer Center Campaign Cybersecurity Playbook
- Harvard Kennedy School Belfer Center Election Cyber Incident Communications Coordination Guide
- Harvard Kennedy School Belfer Center The State and Local Election Cybersecurity Playbook
- National Association of Elections Officials Election Center Elections Security Checklist
- Voting System Technical Oversight Program at Ball State University (VSTOP) Indiana Best Practices Manual for the Operation of Election Equipment
- Voting System Technical Oversight Program at Ball State University (VSTOP) Risk Limiting Audit (RLA) Pilot
- Voting System Technical Oversight Program at Ball State University (VSTOP) Risk Limiting Audit (RLA) Pilot Report

Center for Internet Security (CIS)

Handbook for Elections Infrastructure Security

February 2018

Center for Internet Security®

Version 1.0 February 2018

A Handbook for Elections Infrastructure Security

Center for Internet Security®

About CIS

CIS is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. Our CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities.

Except as otherwise specified herein, the content of this publication is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC-BY-NC-SA-4.0).

https://creativecommons.org/licenses/by-nc-sa/4.0/

Center for Internet Security®

31 Tech Valley Drive
East Greenbush, New York 12061

T: 518.266.3460
F: 518.266.2085

www.cisecurity.org
Follow us on Twitter @CISecurity

A Handbook for

Elections Infrastructure Security

Part 1:
Introduction

Part 2:
Elections Systems and Risk

Part 3:
Mitigating System Risk

https://www.cisecurity.org/elections-resources/

A Handbook for **Elections Infrastructure Security**

Acknowledgments

CIS would like to recognize the following individuals and organizations for their support in creating this handbook. Their time and expertise were invaluable in completing this important work.

CIS authors

Brian Calkin
Kelvin Coleman
Brian de Vallance
Thomas Duffy
Curtis Dukes
Mike Garcia
John Gilligan
Paul Harrington
Caroline Hymel
Philippe Langlois
Adam Montville
Tony Sager
Ben Spear
Roisin Suver

Community contributions to and review of the handbook

Joseph Lorenzo Hall
Center for Democracy and Technology

Noah Praetz
Cook County, Illinois

Adam Ambrogi
Democracy Fund

Mike Goetz
Election Systems and Software

Tim Mattice
The Elections Center

Peter Lichtenheld
Hart InterCivic

Yejin Cooke
National Association of State CIOs

Susan Frederick and Danielle Dean
National Conference of State Legislators

Tim Blute and David Forscey
National Governors Association

Joshua Franklin and Gema Howell
National Institute of Standards and Technology

Emefa Agawu and Ian Wallace
New America Foundation

Tony Adams
Secure Works

Daniel Kambic and Greg Shannon
Software Engineering Institute

Trevor Timmons
State of Colorado

Robert Giles and Kevin Kearns
State of New Jersey

Tom Connolly
State of New York

U.S. Department of Homeland Security

Ryan Macias and Matt Masterson
U.S. Election Assistance Commission

David Mussington
University of Maryland

J. Alex Halderman
University of Michigan

Marian Schneider
Verified Voting

Contributions of current best practices

In addition, we'd like to thank the following individuals and organizations for providing examples of best practices in use today.

Beth Dlug
Allen County, Indiana

Emmit Lamb
Clark County, Nevada

Chris Chambliss
Clay County, Florida

Scott Konopasek
Contra Costa County, California

Kyle Rulli
Douglas County, Colorado

Stan Bethea
Duval County, Florida

Mark Earley
Leon County, Florida

Joe Miller
Linn County, Iowa

Bill Burgess
Marion County, Oregon

Faith Lyon
Portage County, Ohio

Ricky Hatch
Weber County, Utah

Part 1: **Introduction**

How cybersecurity and elections intersect and why it matters.

To enable the elections that define democracy, we must protect the security and reliability of elections infrastructure. Through a best practices approach, we aim to help organizations involved in elections better understand what to focus on, know how to prioritize and parse the enormous amount of guidance available on protecting information technology (IT) systems, and engage in additional collaboration to address common threats to this critical aspect of democracy.

The Center for Internet Security (CIS) and its partners publish this handbook as part of a comprehensive, nationwide approach to protect the democratic institution of voting. Election officials have been working diligently to secure their systems but, like so many other sectors, the threat to national security rises above any individual organization; we can accomplish more together, and we all share the same goal of free and fair elections. To that end, CIS is committed to a long-term effort to continuously advance and promote best practices for elections security as part of a national response to threats against elections infrastructure. This handbook addresses cybersecurity-related aspects of elections systems.

Background and purpose

Elections are the bedrock of democracy. Even before the establishment of the United States, adversaries sought to corrupt, interrupt, or otherwise disrupt democracy by subverting elections. From adversarial nation states, to terror groups, to Boss Tweed vote strikers, to those simply wishing to wreak havoc, attacks on the voting process are as old as voting itself. There is no way around it: protecting democracy calls for protecting elections.

The desire of some to disrupt elections has not changed; Joseph Harris's 1934 seminal book on elections, *Election Administration in the United States,* enumerates a series of election fraud incidents throughout American history. What is different in recent years is some of the tactics of such efforts to undermine democracy. Attacks leveraging weaknesses in digital infrastructure now augment traditional approaches and have become an increasingly common approach.

Judging by activity in industries and sectors outside elections, this should come as no surprise. Organizations across all sectors and government entities alike face daily attacks from actors with widely varying levels of sophistication. The most capable, best protected organizations have specific plans for addressing evolving threats. The plans are never static; these entities continually adapt—as do their adversaries—requiring an ongoing investment in security.

Moreover, in many industries and sectors, the good guys have realized that a go-it-alone strategy isn't enough. They've developed approaches that allow them to share information, establish best practices, and develop coordinated response plans to mitigate effects of coordinated attacks. This collaboration raises the level of security for the individual organizations, their respective industries or sectors, and the country.

Even in the financial services industry—in which annual investments by individual organizations in improved security for their digital systems can range in the many hundreds of millions of dollars—organizations pool some resources to support the Financial Services Information Sharing and Analysis Center. This collaborative approach to monitoring the evolving threat environment helps support even the most substantial individual efforts. These same approaches have been repeated in many industries, including communications, the defense industrial base, aviation, oil and gas, real estate, electricity, and others. Protecting elections infrastructure is certainly no less important to our country's national security and overall well-being than protecting the infrastructures in these other vital sectors.

In the state and local sector, the Multi-State Information Sharing & Analysis Center (MS-ISAC) works with state and local entities to monitor threats to their systems, detect common attacks across states, and support mitigation of risks presented by vulnerabilities and changing attacker behavior. This results in a more rapid deployment of solutions when new threats emerge; if there's one thing we know about these actors, once they succeed in an attack, they'll duplicate it everywhere they can.

The parent organization of the MS-ISAC and sponsor of this handbook, CIS, has used collaboration among a large number of security experts as a means to identify best security practices. These collaborative processes have resulted in several products available to state and local governments and other entities, including election officials and their technical staff. These include the CIS Controls and CIS Benchmarks, which heavily inform the recommendations in this handbook.

An underlying reality to all current work in cybersecurity is that a skills gap exists for cybersecurity globally, across all industries—elections included. Closing this skills gap is critical to elections and securing the process. Implementing best practices is only possible with the right people who have the necessary skill-set. Therefore, we hope what follows in this handbook will serve individuals with differing skills and resources in implementing practical guidance for election administration.

The elections environment

Elections in the United States are highly decentralized with more than 8,000 jurisdictions across the country responsible for the administration of elections. While the federal government provides some laws and regulations, states have substantial discretion on the process of conducting elections. The federal government does not administer elections and has a limited role in dictating how the process is to be conducted.

States act as the primary authority for the laws and regulations that govern the process of conducting an election in that state. Under federal law, states must designate a chief state election official. This official typically sets rules and regulations for the implementation of election technologies and their use. Although states are heavily involved in setting the rules and policies for administering elections, and in choosing election technology, in most states local jurisdictions administer and conduct the processes of an election.

Many local jurisdictions have the ability to procure their own election technology from a set of certified or approved manufacturers and vendors designated by their respective state. Additionally, the local jurisdictions are typically responsible for inventorying, securing, and training staff on those technologies. Depending on the size and resources of the jurisdiction, the number and technical skills of the staff can vary greatly, ranging from an elections team with its own dedicated IT and security personnel to a single person with little to no IT background. Many elections offices rely on IT resources shared with other administrative functions (e.g., other county agencies) or rely exclusively on technology providers (e.g., elections and IT systems vendors) for implementing and securing their election infrastructure. This can result in dependencies that are outside of the local officials' control.

Audience

By using this handbook, we hope election officials and those that manufacture, own, operate, or are otherwise involved with elections systems and their IT components are better able to understand and prioritize risks, understand best practices that can identify threats, detect attacks, allow for recovery from cybersecurity incidents, and, ultimately, continue to provide and support systems for the execution of free and fair elections.

In addition to this handbook providing a path to continually evolving security, perhaps the most important aspect of this effort is to help instill a continued sense of faith in elections by voters themselves. We hope election officials are able to use this handbook to highlight the past and ongoing work they've done to secure the elections process and that, through openness, transparency, inclusion of relevant stakeholders, and consideration of the entirety of the elections process, voters recognize that democracy is working and their votes will count.

More specifically, we hope this handbook is of use to each of the following:

- **Election officials and senior executives.** These individuals are accountable for executing elections. In addition to state and local election officials, they may include those indirectly involved in the election process, such as the offices of legislators and governors.
- **Owners and operators of elections systems.** These individuals have more responsibility for the systems themselves, though there may be some overlap with election officials. It's critical that they understand the risk context and the technical guidance in this handbook.
- **Vendors of hardware and software.** Whether providing systems and services dedicated to elections or general purpose but used in elections, vendors are, and must remain, partners in this process. Moreover, vendors often provide the primary technology expertise and labor to local election officials. Vendors have a vested interest in their products and services, and election officials driving vendors toward best practices can help all boats to rise with the tide, including improvements in the development, testing, and continual evolution of vendors' products.
- **Others who can help secure elections.** This includes the U.S. Election Assistance Commission (EAC), the U.S. Department of Homeland Security (DHS), state chief information officers and chief information security officers, state homeland security advisors, fusion centers, election integrity groups, academics, and other non-profits and private companies willing to lead or support various efforts. This is, in many ways, a baselining effort that we hope supports other efforts dedicated to improving the security of elections, both new and ongoing.
- **Voters, the media, and other interested stakeholders.** In the end, no stakeholder matters more than voters. Not only is it the duty of all to ensure elections represent the will of voters, but it is the duty of all to ensure that voters have confidence in the process before heading to the polls and after results come in.

Goals and outcomes

This handbook is about establishing a consistent, widely agreed-upon set of best practices for the security of systems infrastructure that supports elections. It provides both a general explanation of the threats that exist for the various components of the elections process and examples of known mitigations for these threats.

By developing and publishing this handbook, CIS aims to establish a baseline of protection for all aspects of the elections infrastructure ecosystem that leverage digital tools and applications.
The primary goal of this handbook is to impact and improve the security of elections infrastructure as soon as possible, and ideally in advance of the 2018 elections, and establish a set of best practices that, with continual updates, supports elections infrastructure security into the future. We expect many elections systems will already incorporate the majority of these mitigations, allowing those jurisdictions to demonstrate a strong baseline. In that case, the handbook can assist in prioritizing for continual improvement and evolution.

Handbook structure

This handbook is divided into three parts that together provide a baseline view of how to manage cybersecurity risk in elections:

- **Part 1: Introduction.** This introductory section describes this handbook and providessome general information on risk assessments in elections systems.
- **Part 2: Elections Systems and Risk**. The second part **introduces a high-level generic elections architecture,** some components of which may exist at the state level, some at the local level, some both, and some not applicable in certain jurisdictions. It also **classifies these common components of elections systems according to the manner in which they are connected to networks or other systems.** For each major component of the generic elections infrastructure, there is an overview and description of how it fits in the elections landscape and a brief description of the risks and

threats associated with the component. Finally, it summarizes the classification-based ways that different implementations of the components are connected to other digital infrastructure.

- **Part 3: Mitigating System Risk.** The third part is a **technical best practice guide that provides controls and recommendations for systems.** It includes two major sections: 1) a set of critical risk-mitigating activities that can benefit any organization and 2) a set of technical best practices for users, devices, software, and processes that are listed first for components that are network connected and then for those that are indirectly connected. We also provide technical best practices that address transmission of information among digital components of the elections infrastructure. As described below, the nature of the connectivity to other elements of the elections digital infrastructure is the major security vulnerability area and thus we have chosen this connectivity as the basis for organizing technical controls. Technical staff, whether government or contracted resources, should be able to implement these controls to provide an appropriate mitigation of risk.

What this handbook is not

A shortcoming of many efforts in domains as large as IT security and elections is a failure to properly scope efforts. In addition to describing what this handbook is, we want to be explicit about what this handbook is not.

Aspects of elections, voting, and protecting democratic institutions that are not part of the scope of this handbook are not an indication of importance, but rather an acknowledgment that no single effort can successfully address everything. This handbook limits its scope to only digital aspects of elections themselves, though in some cases it references paper-based processes in order to further the discussion. The one exception to this is the recognition of how the means of transmission can inject cybersecurity risks, such as digitally transmitting to-be-paper pollbooks to a printer. In these cases, we identify the transmission risks in Part 2 and the mitigations to transmission risks in Part 3.

Beyond this, there are several aspects of election security we do not address. This handbook is not:

- **A one-size-fits-all.** This handbook **does not recommend any single approach to managing election systems or developing and deploying elections systems technology.** Election jurisdictions tailor their voting processes and systems to the needs of their voters and jurisdictional laws and requirements. That said, there are many commonalities. Rather than focus on differences of approach, this handbook focuses on the best practices associated with common approaches, recognizing the variety of approaches and architectures wherever possible.
- **An all-encompassing scope.** As this handbook is about improving the security of elections infrastructure as it exists today, **we have intentionally left several aspects of the broader voting process, however important, out of scope:**
  - Eligibility for an individual to register to vote;
  - Voter identity verification, unless specifically about the accuracy and availability of voter registration rolls;
  - Security of campaigns or campaign information systems; and
  - The accuracy of information about candidates or issues, including those conveyed using social media.

Assessing risk in elections systems

A common way of describing an organization's cybersecurity posture is in terms of risks that have been mitigated and risks that have been accepted. Those outside the information security community will often think of security in terms of stopping all possible threats. Both within the community and in the legal domain, practitioners understand that perfect cybersecurity is not possible. Rather, organizations seek to achieve "reasonable" security that involves accepting some level of risk given the threats and potential consequences, while maintaining an ability to recover should any of those consequences be felt.

Elections systems risk overview

The IT systems infrastructure that supports our elections processes has myriad risks, and these risks vary from one organization to the next. There are a number of commonly used risk assessment approaches that can be used by election officials and their technical staff to help assess risk, such as International Organization for Standardization (ISO/IEC) 27005 and National Institute of Standards and Technology (NIST) Special Publication 800-30. Among the most popular tools for understanding and managing cybersecurity risk is the NIST Cybersecurity Framework, which organizes cybersecurity activities in five functions: identify, protect, detect, respond, and recover.

Unfortunately, many election officials do not have the expertise or resources to conduct an adequate risk assessment. The ability to efficiently and effectively execute a risk assessment is further reduced by the difficulty in objectively assessing evolving threats, as well as the complexity of the elections processes and systems.

In its simplest form, a risk assessment is used to identify and assess the impact of vulnerabilities—weaknesses that an attacker can exploit—while being mindful of the compensating controls that exist in a system. These risks can be mitigated with appropriate physical, process, and technical safeguards. In this way, risk and potential impacts can be reduced to a level deemed acceptable by the accountable election officials, often called a balanced risk posture. The potential impact or consequence of a successful exploit is an important part of a risk assessment as elections officials want to focus first on exploits that have the greatest potential consequence. While some risks vary from one election jurisdiction to another, many are common across the wide variety of elections systems configurations. As part of producing this handbook, experts have collaborated to assess the common risks to elections systems. This common baseline risk assessment has influenced the prioritization of security best practices in the handbook.

Baseline elections risk assessment

The baseline assessment of risk for elections is summarized for the purpose of helping election officials and their technical staffs understand the major areas of risk that can serve as their primary focus. Each organization should augment the baseline elections risk assessment to address the risks that might be unique to their elections processes, systems, and threats.

Examples of threats and consequences

Scenario 1:
A nation-state uses the internet to access and disrupt one or more state voter registration databases such that legitimately registered voters are denied the ability to vote on election day, or are required to file a provisional ballot.

Consequence:
Although no votes are manipulated, this attack would likely be a major national news story that results in reduced confidence by the public in the integrity of the voting process and the election results. Additionally, this slows the voting process, creating the risk of long lines and making in-person voting less efficient.

Scenario 2:
An adversary gains access through the internet to one or more election night vote displays and changes the displayed results such that the real winner of the election is now the reported loser in the election.

Consequence:
Again, while no votes have been changed, and the erroneous posting of election results by an authoritative source will subsequently be republished correctly, there is likely to be a significant loss of voter confidence.

A top-level assessment of vulnerabilities and potential consequences to the elections systems infrastructure identifies network connectivity—devices or systems that work with other devices or systems to achieve their objectives—as the major potential vulnerability. The reason is simple: given an adversary with sufficient time and resources, systems that can be accessed via a network cannot be fully protected against compromise. There are ways to improve the security of network connected systems with additional controls, but the inherent complexity of network connectivity results in significant residual vulnerabilities.

Therefore, risks for system components that are connected to a network should be treated differently than for components that are never connected to a network. In this handbook, the definition of "network" includes connections to the internet as well as connections to both local wired and wireless networks.

While systems that are continuously connected to a network have a somewhat higher risk than systems that are only intermittently connected to a network, experts have demonstrated that any network connectivity, even if only for a limited period of time, results in a significantly larger vulnerability profile. An access path to these components may be available through the internet if any connected component can access the internet, and thus an attack can be orchestrated from anywhere in the world. The box to the right illustrates examples of these threats.

On the other hand, systems that have a digital component but are not network connected have a reduced vulnerability profile. Specifically, there are fewer ways to attack such systems and devices, but it does not mean the consequences of a successful attack are any lower—indeed, an attack can still be executed without geographic boundaries. The methods used to upload and download information (e.g., USB sticks, memory cards) still have vulnerabilities, but there are fewer vectors of attack to mitigate.

Three classes of elections systems

In this handbook, we have organized best practices into two classes based on the different threat characteristics associated with levels of connectedness. A third class, that of processes that are executed without a digital component, such as hand-counted paper ballots—the casting and counting of ballots via purely paper and manual means—is out of scope for the handbook.

While there are many components to a complete election system, many of the cybersecurity risks associated with them can be grouped to simplify the steps to manage risk. One approach to this is by analyzing the manner in which they connect to networks and other devices. Throughout this handbook, we classify components of elections systems based on three types of connections that most clearly define the risk landscape:

1. **Network connected systems and components.** Network connected components are interconnected with other devices to achieve their objectives. The level of interconnection, while providing various benefits, also introduces additional risks that must be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means for accessing and managing the devices, which means organizations must make extra efforts to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet, nor does their connection have to be persistent. As an example, an Election Management System (EMS) connected to a private county network would still be classified as a network connected system.

2. **Indirectly connected systems.** Indirectly connected components are not connected to a network at any time and are not persistently connected to other devices. They do, however, have to exchange information with other elections system components including network connected systems in order to complete their objectives in the election process. These information exchanges are done using removable media such as USB drives or other flash media. While the risks associated with being connected to a network or the internet are no longer relevant, threats are introduced by exchanging information with other devices, either through the use of removable media or a direct connection to another device such as a printer or an external disk drive.

3. **Non-digital elections components.** These are aspects of the elections process that have no digital component and are **out of scope for this handbook.** An example would be the mailing, completing, and returning of a paper mail-in ballot. While aspects of the overall process—such as an online request for the ballot—may leverage digital infrastructure, the aspect of this process that is purely paper-based is out of scope.

In Part 2 of the handbook, each major component of an election system is briefly described and then placed into one of these classes, providing a method to simplify the risk landscape and assist officials and their technical staff in determining the most effective and efficient approaches to managing risk. In some cases, major components are divided into the primary approaches to executing a process, such as the different approaches to conducting vote capture, each of which is classified individually. This classification analysis becomes the foundational basis for an elections organization selecting the appropriate technical best practices for that component described in Part 3 of the handbook.

Transmission between components creates vulnerabilities

While securing elections systems components is important, one of the largest sources of vulnerabilities, and thus most common methods of attack—attack vectors in cybersecurity parlance—lies not in the systems but in the transmission of data between systems. Weaknesses in communications protocols, or in their implementation, risk exposure or corruption of data, even for systems that are otherwise not network connected. For instance, while paper pollbooks wouldn't typically have cybersecurity risks, if the data for the pollbooks is sent electronically to a printing service, this transmission introduces risks that must be addressed. Similar vulnerabilities exist in transmission of ballot layout information to printers or in loading ballot information into ballot scanning (i.e., vote capture) devices. In Part 3, we also address transmission risks of this nature and the best practices that can mitigate them.

Part 2: **Elections Systems and Risk**

A description of major elections components and their risks.

This part of the handbook provides a generalized elections systems architecture showing each major component of the systems and:

1. A discussion of the risks and threats for each major component,
2. For some components, a description of the different types of deployment in use, and
3. A classification of the component based on how it connects to other devices, and thereby a mapping to controls and recommendations in Part 3 of this handbook.

A generalized elections systems architecture

There are many flavors of elections infrastructure, both from a technology and a process perspective. This is true far beyond just the different types of vote capture and vote tabulation devices. That said, many experts have studied the elections process at length, and there are several fundamental components common to nearly all elections systems.

In some jurisdictions, the owner of various aspects of the architecture may differ, but the fundamentals of the types of systems used to perform the task are generally the same. For that reason, many of the best practices associated with those systems will closely follow IT security best practices. Those accountable for elections infrastructure should understand these basic processes and identify the parts where they have purview. A description of major system components that comprise the elections infrastructure are shown in [FIGURE 1].

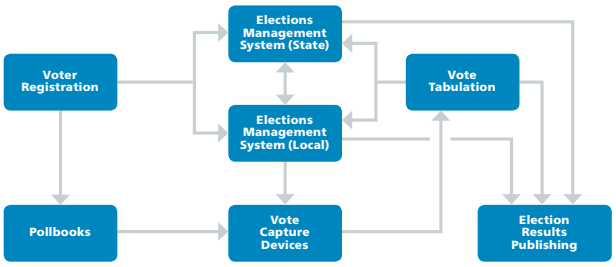


FIGURE 1: *A generalized elections systems architecture*

While each of these systems has IT components that require security best practices, this handbook addresses a subset that are, in our view, the highest risk targets of attack by adversaries and thus require the bulk of the attention. For digital components not covered in the handbook, the analysis methods used here can be applied to determine the appropriate set of technical best practices for that component.

Many of the components in elections infrastructure are built on general purpose computing machines, such as traditional web servers and database platforms. While this means they are often subject to the same attacks as those in other sectors, it also means experts have identified best practices to mitigate many of the risks.

Each of these components may exist at the state level, at the local level, or both, and some will not be applicable in certain jurisdictions. Nonetheless, all will exist in most jurisdictions and must be addressed in order to provide a comprehensive best practices guide. This is especially true for local jurisdictions, given the extent to which elections are administered locally. Even where there is a substantial amount of legacy infrastructure—old systems that are difficult or impossible to update—much can be done to mitigate risks. These systems are described below and appropriate best practices and controls are provided in Part 3.

Voter registration

Every state has a unique approach to voter registration—including some states with automatic voter registration—but there are several commonalities shared by all of them. Voter registration systems provide voters with the opportunity to establish their eligibility and right to vote, and for states and local jurisdictions to maintain each voter's record, often including assigning voters to the correct polling location. Voter registration systems support pollbooks—paper and electronic—as well as provide information back to the voter as they verify their registration and look up polling locations and sample ballots.

The inputs to voter registration systems are registrations, removals due to ineligibility (e.g., an individual moving out of state, death of a voter), and record updates, most often due to an individual moving within the state. The outputs include facilitating voter lookups—such as a voter verifying they are registered, seeking a sample ballot, or finding their polling place—and transfer of voter information to pollbooks.

In all of these cases, there is a master voter database at the state level. The 2014 EAC Statutory Overview describes this database as populated in one of three broad ways:

1. A top-down system in which the data are hosted on a single, central platform of hardware and maintained by the state with data and information supplied by local jurisdictions,
2. A bottom-up system in which the data are hosted on local hardware and periodically compiled to form a statewide voter registration list, or
3. A hybrid approach, which is a combination of a top-down and bottom-up system.

For all three cases, voter registration systems consist of one or more applications that leverage general-purpose computing systems built on commercial-off-the-shelf (COTS) hardware and software. Because they use these common computing platforms, voter registration systems may be part of a shared computing system, though in many cases they are dedicated systems with dedicated software.

While jurisdictions vary in how they allow voters to apply or update their registration, in many states, the most common way voters access a registration system is through the state's department of motor vehicles (DMV).

Additionally, voters' connection to the voter registration system may run through direct means such as a county or state registration portal, or through indirect means like mailing in a registration on paper. To address this risk, many voter registration systems with which the voter would

interact are separated from the "official," or production, voter registration system. Periodically, a report of changes is generated and undergoes a quality assurance review that must be certified before being entered into the production system. This can substantially reduce, for instance, an online portal as a vector of attack, though the production system may still be network connected in other ways.

In general, voter registration systems exhibit the risk characteristics of a general-purpose computing system and, more specifically, any network connected database application. To properly mitigate risks, each voter registration system within a state, and links to the voter registration system, needs a comprehensive assessment of its technical characteristics and the application of appropriate security controls.

[FIGURE 2] shows the major functions or subsystems of a voter registration system.

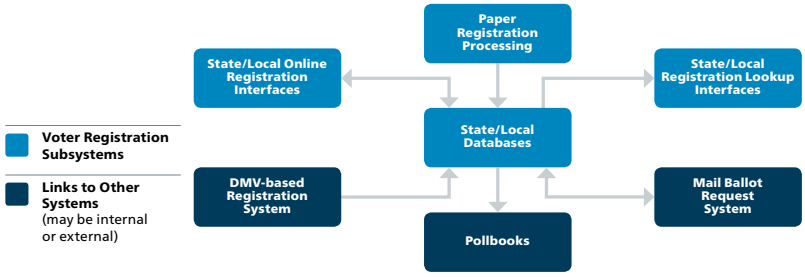


FIGURE 2: *Components of a typical voter registration system*

Types of voter registration

Voter registration generally occurs in one of two ways, each of which is recorded in a statewide registration system.

1) **Online registration:** a website or other web application allows prospective voters to register electronically and have election officials review their registration for validity, which, if valid, is entered into the voter registration database. Same-day registration, because of the need for live updating and cross checking, usually falls into this category.

2) **Paper-based registration:** prospective voters submit a paper voter registration form that is reviewed by election officials and, if valid, entered into the voter registration database. Registration of this type is out of scope in this handbook.

The type of voter registration employed at DMVs will vary by state—and perhaps locality—but should typically be viewed as a form of online registration.

Risks and threats

As noted in the previous section, the ability to access voter registration systems through the internet results in a significant increase in vulnerability and resulting risk. There are well known best practices to mitigate these risks such as those described in the box to the right, but the ability to attack and manipulate voter registration systems by remote means makes them a priority for strengthening of the security resilience of these components.

While the attacks on voter registration systems may have a specific purpose not found outside the elections domain, the vectors for those attacks, and thus the primary risks and threats associated with voter registration systems, are similar to those of other systems running on COTS IT hardware and software, and include:

- Risks associated with established (whether persistent or intermittent) internet connectivity,

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

These items must be managed to ensure proper management of voter registration systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats. Based on their type of connectedness to digital systems, these controls are listed in Part 3.

In practice: protecting the voter registration database

Cybersecurity practitioners constantly face a difficult balance between convenience for users and strong security. With voter registration databases, some approaches allow elections officials to have it both ways.

Practice #1:
Officials in Washington State leverage what's called a "sneakernet" to move information from an internet-facing copy of the voter registration database and a master version of the database that is not connected to the internet. Officials have to physically move data from one machine to another—usually by moving their sneakers to walk it across the room. This doesn't eliminate all risks, but can help protect sensitive information from attack through internet-based vectors, while still allowing individuals to access their information over the internet.

Officials can only access the database from a special application. This application makes periodic copies of the database in a tightly controlled environment and these copies are used to populate all other interfaces. Similarly, changes to the master database are limited to this application. So updates from, say, the DMV don't directly access the database. They're carefully checked for corruption and moved to the master database through this controlled process.

Practice #2:
Some jurisdictions don't air gap their master voter database but use other methods to balance strong security and real-time election official access to the database. In Colorado, the master database is accessible via networks due to needs such as facilitating same-day registration. Experienced cybersecurity professionals leverage appropriate protections including strong vulnerability and risk management programs coupled with robust access controls, intrusion detection and prevention systems, web application firewalls, and security information and event management integration. Multiple layers of defenses—both computerized and human—are used to sustain operations while minimizing risk.

How these components connect

Each type of voter registration, along with the master voter registration database, should have risks evaluated individually based on its type of connectivity and employ controls and best practices found in Part 3 that correspond to the type of connectivity and are appropriate to address risks. That said, aspects of the voter registration systems, and the types that may be implemented, have general characteristics that can be classified by connectivity. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

1) Online registration.

In addition, the master registration database or system itself should be considered network connected.

Indirectly Connected

N/A

Not connected, out of scope

2) Paper-based registration.

Additional transmission-based risks

Transmission of a registration via email or fax leverages a digital component and should incorporate the relevant transmission-based mitigations in Part 3.

Pollbooks

Pollbooks assist election officials by providing voter registration information to workers at each polling location. Historically, these were binders that contained voter information and could be used to mark off voters when they arrived to vote. While paper pollbooks remain in use today, many pollbooks are electronic and aim to facilitate the check-in and verification process at in-person polling places. While this section focuses primarily on electronic pollbooks (e-pollbooks), it also recognizes that, depending on the implementation, producing paper pollbooks can carry transmission-based risks.

These e-pollbooks play a critical role in the voting process. They are necessary to ensure voters are registered and are appearing at the correct polling place, and their efficient use is necessary to ensure sufficient throughput to limit voters' wait times. These e-pollbooks are typically dedicated software built on COTS hardware and riding on COTS operating systems.

The primary input to e-pollbooks is the appropriate portion of the registration database. The primary output is the record of a voter having received a ballot, and in some cases providing a token to activate the vote capture device. In some cases, for instance where same-day registration is permitted, e-pollbooks may require additional inputs and outputs to allow for election day changes.

Paper pollbooks are produced from digital records, including digital registration databases. Having taken appropriate measures to mitigate risk for voter registration components, secure transmission of voter information to a printer—whether at the state or local level, or via commercial printing services—protects the integrity of the information in printed pollbooks.

Risks and threats

Attacks on e-pollbooks would generally serve to disrupt the election day process by one of these three situations: 1) attacking the integrity of the

data on the pollbook by altering the information displayed from voter rolls, 2) disrupting the availability of the e-pollbooks themselves, or 3) in some cases, causing issues with the vote capture device by altering an activation token. Any of these situations could result in confusion at the polling locations and likely a loss of confidence in the integrity of election results. A successful attack of the first variety would more likely occur in voter registration systems by deleting voters from rolls or subtly modifying information in a way that prevents them from casting a ballot or forces them to use the provisional ballot process, but could also occur in the e-pollbooks themselves and during the transmission of data to the e-pollbook.

An e-pollbook may or may not be connected to a network. If they are network connected, they must be treated as having the risks of a network connected device, even if the functionality is not used. While threats are continually evolving, appropriate measures can be taken to address this largely known set of risks.

The primary cybersecurity-related risks to paper pollbooks come from the transmission of pollbook data to formatting and printing services. Data will typically be loaded onto an e-pollbook through a wired connection, a wireless network, or removable media such as a USB stick. To that end, risks and threats include:

- Risks associated with established (whether persistent or intermittent) internet connectivity,
- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities, including private networks for e-pollbooks,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in the dedicated components, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users, including permissions for connecting to networks and attaching removable media, and
- Difficulty associated with finding, and rolling back, improper changes found after the fact.

These primary risks must be managed to ensure proper management of pollbooks. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats.

How these components connect

Managing risks associated with e-pollbooks will generally fall into one of two classifications based on the way they can connect to load data and, if applicable, transmit data. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected
Pollbook connects via a wired or wireless network.

Indirectly Connected
Pollbook connects via a physical media connection or removable media (e.g., USB sticks and other flash media that are physically connected and disconnected to other devices).

Not connected, out of scope
Paper-based pollbooks.

Additional transmission-based risks
Transmission of data for paper-based pollbooks for formatting or printing. If this transmission incorporates a digital component, it should incorporate the relevant transmission-based mitigations in Part 3.

State and local Election Management Systems

States and local jurisdictions generally have established, persistent Election Management Systems (EMSs) that handle all backend activities for which those officials are responsible. Each state has an EMS, and each local jurisdiction will typically have a separate EMS that may, but will not always, connect to the state's system. The extent to which the two systems are integrated, if at all, varies greatly.

For the most part, a local EMS is used to design or build ballots, program the election database, and report results. A state EMS typically does a wide variety of things including election night reporting and military and overseas ballot tracking.

An EMS will also typically include vote tabulation. For the purposes of this handbook, vote tabulation is broken out into its own section.

EMSs can have a wide variety of inputs and outputs that will depend on the separation of duties between the state and the local jurisdictions and the manner in which each state or local jurisdiction handles particular aspects of the election process.

Risks and threats

While EMSs are typically dedicated software that carries its own risks, that software generally runs on COTS software and hardware that operate in a networked environment. Many risks and threats associated with EMSs are similar to those of other systems running on COTS IT hardware and software, and include:

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in the dedicated components, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

Significant consequences may result from successful attacks on an EMS. These potential consequences include the inability to properly control election processes and systems or, depending on the functions of the EMS, incorrect assignment of ballots to their respective precincts or other errors. Furthermore, successful manipulation of an EMS could result in cascading effects on other devices that are programmed from the EMS, potentially including voting machines and vote tabulation.

How these components connect

The diversity of functions delivered by an EMS makes it difficult to generalize the level of connectedness of any given system, but most will have at least some aspects of a network connected system. A host of factors impact connectedness, such as whether a state or local EMS is network connected and whether communications with the EMS leverages connections such as a Secure File Transfer Protocol (SFTP). Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected
Unless known definitively to have no network capabilities, treat an EMS as network connected.

Indirectly Connected
If known definitively to have no network capabilities, treat an EMS as indirectly connected.

Not connected, out of scope
N/A

Additional transmission-based risks
N/A

Vote capture

Vote capture devices are the means by which actual votes are cast and recorded. Approaches vary greatly both across and within jurisdictions. Any given jurisdiction, and even a single polling place, is likely to have multiple methods for vote capture to accommodate both administrative decisions and different needs of voters.

For instance, on election day, a polling place may give voters the choice of electronic machines or paper ballots. Another instance, voters with language needs or voters with disabilities may necessitate the use of additional components or a separate device.

To this end, providing specific recommendations around vote capture security is a detailed task. The EAC, in coordination with other federal partners, state and local governments, vendors, and others in the elections community, maintain standards and a certification program for vote capture devices. We will not try to replicate or alter those recommendations here, but we will provide a generalized set of recommendations that can help guide officials toward best practices for vote capture devices.

Vote capture devices are often top of mind when thinking of election security—and for good reason. Vote capture devices are where democracy happens: the voices of the people are heard via the ballots they cast. But, as documented throughout this handbook, they are a single part of a larger ecosystem for which a holistic security approach is necessary. Much attention has been paid to vote capture devices, and these efforts should continue; ensuring the security of vote capture devices, like any aspect of security, is a continuous process.

The primary inputs to vote capture devices are the ballot definition file—which describes to the device how to display the ballot—as well as an activation key (for some electronic machines) and the ballot itself for scanning of a paper ballot. The primary output is, of course, the cast vote record.

In cybersecurity, we often talk about non-repudiation: the inability to deny having taken an action. Our democracy is founded in the opposite principle: your ballot is secret; no one should be able to prove who or what you voted for—or against—in the voting booth. This presents an inherent difficulty in maintaining the security of the voting process. We intentionally create voter anonymity through a breakpoint between the fact that an individual voted and what votes they actually cast. We never want to enable the ability to look at a marked ballot and track it back to a specific voter.

Instead, we must carefully protect the integrity and secrecy of the vote cast through the capture process and into the process of tabulation. To do this, best practices call for applying a series of controls to mitigate the risk that a vote capture device is functioning improperly, to identify problems if they occur, and to recover without any loss of integrity.

Principles and more through the VVSG

The EAC is currently in the process of developing the Voluntary Voting System Guidelines (VVSG) version 2.0. The draft recommended by NIST and the EAC's Technical Guidelines Development Committee incorporates many of the best practices described within this handbook, such as auditability, access controls, data protection, system integrity, and detection and monitoring. The recommended draft is written as a high-level set of principles and guidelines, allowing specific requirements to change without requiring the full EAC approval process. This provides nimbleness and flexibility in voting systems and their underlying cybersecurity as requirements can be developed and mitigations implemented as threats are identified. More information about the VVSG 2.0 development and proposed draft can be found on the EAC's website.

Types of vote capture processes

Vote capture generally occurs in one of six ways:

1) **Voter marked and hand counted paper balloting.** Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, collected, and counted by hand. Hand counting represents a relatively small share of total votes. This category usually covers some mail-in ballots.

2) **Voter marked paper balloting with scanning.** Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, and collected. Votes are tabulated by scanning the paper ballot with an optical or digital scanner, either individually or in batches. This category covers some mail-in ballots.

3) **Electronic marking with paper ballot output.** Rather than handing out a paper ballot, the voter is directed to a machine that displays the ballot. The voter casts votes, and the machine prints a marked ballot. These printed ballots are tabulated either individually or in batches. Votes are usually tabulated by scanning the paper ballot with an optical or digital scanner, though are sometimes counted by hand. The vote capture device does not store a record of the vote selections. This type of vote capture device is commonly referred to as a *ballot marking device.*

4) **Electronic voting with paper record.** The voter is directed to a machine that displays the ballot. The vote is captured on the machine and either transmitted digitally to a central machine for tabulation, or removable media is extracted from the machine at a later time to transmit a batch of captured votes. At the time the vote is captured, the machine creates a printed record of the vote selections that the voter can verify. That record remains with the machine. This type of vote capture device is commonly referred to as a *direct record electronic (DRE) device with voter verifiable paper audit trail.*

5) **Electronic voting with no paper record.** The same as electronic voting with paper record, but the machine does not print a record of the captured vote. Captured votes are only maintained digitally, typically in multiple physical locations on the device and, sometimes, on a centrally managed device at the polling location. This type of vote capture device is commonly referred to as a *DRE device.*

6) **Electronic receipt and delivery of ballots conducted remotely.** The majority of ballots received by voters using this method are voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). Though most UOCAVA votes involve paper ballots, there is a sub-set of this population that submits their marked ballot in a digitally-connected method such as email or fax. Once received digitally, the voter's vote selections are transcribed so that the vote selections are integrated into the vote tabulation and results reporting systems; these systems do not have network connections to the voting system. When this approach is used, the balloting itself is out of scope as it is via paper means. However, this type of voting can carry transmission-based risks.

Risks and threats

The consequences of a successful attack in a vote capture device are significant: the intentions of a voter are not properly reflected in the election results. The vast majority of vote capture devices are not network connected systems. This helps limit the attack paths and therefore the risks to which they are subject—in cybersecurity parlance, a non-networked approach substantially reduces the attack surface. Therefore, to change a large number of votes typically requires access to the vote capture machine hardware or software, or the ability to introduce errors through the devices that program the vote capture device or download results from the vote capture device. Moreover, most vote capture devices are tested and certified against criteria defined by the EAC, a state or local entity, or both, though evolving threats can change the risk profile of a device even if it has previously been certified.

The type of vote capture device we call *electronic receipt and delivery of ballots conducted remotely* can take on a large number of flavors. In terms of cybersecurity-related risks, for activities like emailing ballots, election officials must consider especially risks involved in the transmission of the ballot. Whether during distribution or return, if the transmission of the ballot is done via digital means, it is subject to the risks of that transmission mode. In Part 3, there is a set of control measures that provide mitigations for risks in transmission.

Regardless of approach, risks exist, and they mostly stem from the transfer of data to or from vote capture machines. Specifically, they include:

- If ever networked, risks associated with established (whether persistent or intermittent) network connectivity,
- Risks associated with the corruption of removable media or temporary physical connections to systems that are networked,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users, and
- Difficulty associated with finding, and rolling back, improper changes found after the fact, especially in the context of ballot secrecy.

How these components connect

Each type of vote capture process should have risks evaluated individually based on its type of connectivity. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered *network connected.*

Although many jurisdictions program the vote capture devices with the ballot definition using indirectly connected methods, some use methods to load the ballot definition files to the vote capture device by transmitting the data over a closed-local area network.

Also, many central count scanners, used for *Voter marked paper balloting with scanning* in batches (usually vote by mail ballots) are similarly networked on a closed-LAN.

Some electronic vote capture machines also directly transmit data for election night reporting.

Indirectly Connected

2) *Voter marked paper balloting with scanning.* Paper ballots do not include an electronic component. While scanners are not typically network connected devices, they must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device.
3) *Electronic voting with paper ballot output.* In addition to the role of the scanners, the vote capture machines are typically not network connected, but must be programmed to display the ballot and print the ballot in the correct format.
4) *Electronic voting with paper record.* The vote capture machines are typically not network connected but must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device.
5) *Electronic voting with no paper record.* The vote capture machines are typically not network connected but must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device.

NOTE: If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered *network connected.*

Not connected, out of scope

1) *Voter marked and hand counted paper balloting.* Out of scope in this handbook as the vote capture process does not include a digital component.

Additional transmission-based risks

6) *Electronic voting conducted remotely.* These methods vary greatly and must be addressed on a case-by-case basis. At minimum, when web-based, email, or fax transmission is used in either direction, it leverages a digital component and should incorporate the relevant transmission-based mitigations in Part 3. Aspects definitively executed without a digital component are *not connected, out of scope.*

Vote tabulation

In its broadest definition, vote tabulation is any aggregation or summation of votes. Vote tabulation is the aggregation of votes (e.g., cast vote records and vote summaries) for the purpose of generating totals and results report files. For the purposes of this handbook, this section on vote tabulation is considered separately from both the EMS of which tabulation is usually a part, and vote capture machines that also tabulate (or aggregate). Vote tabulation in this handbook is focused on tabulation occurring across precincts, counties, etc., and covers both official and unofficial vote tabulation.

Risks and threats

Similar to vote capture devices, attacks on vote tabulation would seek to alter the counting of cast votes. This impact would be felt through the determination of the election outcome as well as the potential for confusion if initially reported outcomes did not agree with later certified results.

Vote tabulation typically involves either dedicated software or COTS software running on COTS hardware and operating systems, though some dedicated hardware is also in use. Vote capture devices most often transmit the vote data (e.g., results, cast vote records) to the vote tabulation system using removable media, though sometimes that data is transmitted across a network. Vote data is most often transferred across jurisdictions and to the state through uploads via direct connections such as a virtual private network, local network connections, faxes, or even phone calls.

The primary risks to vote tabulation are similar to those of other COTS-based systems: a compromise of the integrity or availability of aggregated votes totals could reduce confidence in an election, if not alter the outcome. Though the vote data is likely loaded to these systems via removable media, most risks stem from vulnerabilities in these networked systems themselves. Such risks and threats include:

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,

- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Lack of confidentiality and integrity protection for transmitted results,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

These primary risks must be managed to ensure proper management of vote tabulation systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats.

How these components connect

Depending on the implementation, these systems should be considered network connected or indirectly connected. They may interface with the internet, and, even if they do not, almost certainly interface with a system that is connected to a network. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

In some cases, vote tabulation equipment will be *network connected,* whether through a wired or wireless connection.

Indirectly Connected

If vote tabulation equipment is not *network connected,* it is indirectly connected through removable media.

Not connected, out of scope

N/A

Additional transmission-based risks

N/A

Election results reporting and publishing

After votes are tabulated, results must be communicated both internally and to the public. In any given state, this can take many forms, but, in most cases, the basic process goal remains: getting results as quickly and accurately as possible. This section focuses on election night reporting, which involves unofficial results.

The inputs to election results reporting and publishing tabulated votes as described in the previous section. The systems used for reporting and publishing are likely networked, and, in many cases, have public facing websites.

The outputs are the unofficial election results, typically published on a website, often in multiple formats such as extensible markup language (XML), hypertext markup language (HTML), portable document format (PDF), and comma-separated values (CSV). There is likely a direct and persistent network connection between the published site and the internet, though the official record of the results may be kept on a system that is not persistently connected to the internet.

How these components connect

Depending on the approach to submitting tabulated votes, the reporting component may be network connected. The publishing component is almost certainly network connected, but may be indirectly connected, depending on the implementation. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

In some cases, election night reporting will be n*etwork connected,* whether through a wired or wireless connection.

The publishing component of election night reporting is almost certainly *network connected,* whether through a wired or wireless connection.

Indirectly Connected

If the election night reporting process is not network connected, it is indirectly connected through removable media.

Not connected, out of scope

N/A

Additional transmission-based risks

N/A

Part 3: **Mitigating System Risk**

Critical activities and best practices in elections infrastructure security.

Mitigating risk is, ultimately, about decisions and actions that establish trust in aspects of a system, leading to confidence in the outcome. Risk must be considered at every stage of a system – requirements, design, development, operation, and even for disposal or retirement (e.g., removal of sensitive information).

Like many systems, for election systems this involves establishing trust in users, devices, software, and processes. Many systems are "composed," or built up from a variety of commercial and purpose-built parts, devices, and software connected via processes and user actions. The results in security decisions about trust are made across many components and brought together at a system level. In other cases, key election system components or services functions are contracted out. This does not change the security responsibility for decision-makers, but forces them to think about how the desired security properties can be specified in contract language and service specifications, rather than implemented directly.

This part of the handbook contains:

1. A set of critical risk-mitigating activities from which all organizations can benefit,
2. Recommendations for best practices in contracting for IT services, and
3. A set of best practices in the form of recommendations and controls for network connected and indirectly connected devices, as well as for transmission of information.

Critical risk-mitigating activities

Auditing

Election officials conduct many audits of all aspects of the election process (e.g., vote by mail processing, training, equipment delivery) and election systems (e.g., voter registration transactions, audit log data). However, the focus of this section is on auditing vote capture and tabulation in an election.

Included in this is to validate that the aggregated results reflect the actual ballots cast. One auditing approach is to select a sample of the ballots and, applying a structured process, do a partial recount of the ballots. This controlled audit is intended to provide confidence that the voting results are accurate based on the results of that partial recount. Moreover, audits provide information to election officials that go beyond the requirements for audit and recounting results; audits are the "production time" opportunity for election officials to know that the systems they are using are working properly.

The approach to auditing can vary based on a number of factors, including requirements that may be established within elections jurisdictions. Some auditing requirements call for a manual recount of a set percentage of ballots, others—including risk limiting audits described below—leverage statistical methods to determine the extent of the recount. Auditing requirements typically also have a trigger for a larger recount or full recount based on the outcome of the initial audit. Given the potential expense of auditing, it is critical to properly design audit procedures to reduce costs while achieving the goals of the audit.

Objective auditing in Linn County

In Iowa, Linn County Election Services hired a cybersecurity firm to conduct an audit of various aspects of the county's elections infrastructure. The firm submitted recommendations, and the county decided which of those to prioritize for implementation. The goal in hiring a third-party vendor was to provide objective, professional advice and assistance. This helps ongoing security efforts and gives confidence to the public that Linn County is taking cybersecurity seriously in its elections.

Almost all states have provisions for a full recount of a contest should the result of that contest fall within the state required recount margin (for instance, many states require a recount for a statewide race if that race is within one half of one percent after certification).

The initial audit size and recount triggers are critically important to a good audit. As important is the method by which the audited ballots are selected. Establishing proper methods for random selection of ballots can have a tremendous impact on the audit's ability to confirm election results or show evidence of tampering.

For election officials, the first step to a good audit is recognizing that records must be kept in order to make an audit possible. This means allocating resources to support an audit, along with procedures for efficiently executing the audit and making it sufficiently transparent for interested parties. While audits are not inherently digitally-based efforts, establishing an audit process, with resources, ballot selection methods, audit size rules, and recount triggers, is a critical aspect of mitigating risk across all aspects of elections.

A best practice: risk limiting audits

A possible weakness in some traditional auditing methods is that often either more ballots or fewer ballots are recounted than necessary to validate the results. This can either produce an audit that doesn't fully validate the outcome of the election, or an audit that is more costly than necessary without increasing confidence in the results.

More recently, the concept of risk limiting audits has been introduced as an approach to auditing election results that is both effective and efficient. In addition to those characteristics necessary in a traditional audit—resources, good ballot selection methods, and prior-determined rules—in a risk limiting audit the size of the audit and recount triggers are based on a "stopping rule" determined by the likelihood that the actual election outcome differs from the reported outcome. Put another way, additional ballots are recounted in the audit until there is a pre-determined statistical level of confidence that the reported result is correct. As an example, a very large margin of victory will typically result in a relatively small audit size, as a very large error would have to occur to change the outcome. A very close election, on the other hand, would require a larger audit.

In practice: risk limiting audits in Colorado

Recently, the state of Colorado established a legal requirement that all elections be subjected to a risk limiting audit. The Colorado Secretary of State defines the "risk limits" for each election. The risk limits (i.e., the acceptable probability that the election results might not be correct based on the statistical analysis process implemented within the risk limiting audit) will guide the process of selecting the size and distribution of the sample to be subjected to the initial audit, and in turn successive audits if they are required to achieve the risk limit confidence. The trend of leveraging risk limiting audits continues to gain steam, and election organizations should consider Colorado as a use case from which they can learn. The References section of this handbook provides additional information on Colorado's approach.

In a risk limiting audit, the size of the audit is determined by the results of the audit itself. That is, the closer the audited results are to the actual outcome, the sooner the audit ends. This is termed the statistical confidence in an election's results. As soon as a previously-determined confidence threshold is met, the audit can stop. As in all audits, units—precincts, machines, batches of paper records—should be selected using random sampling methods. In a risk-limiting audit, the sample size will depend on the margin of victory and other factors; these other factors may include the number of ballots in each precinct and the overall number of ballots in the contests. In general, smaller margins of victory and fewer total votes cast require auditing a larger percentage of the ballots cast. These methods are well-documented and replicable through sources such as ElectionAudits.org.

Incident response planning

Despite the best efforts of election officials and their technical staff, there is some likelihood that there will be an incident at some point during an election cycle. This is the nature of cybersecurity; the true measure of success is often the resiliency of an organization in the face of these incidents.

Incidents can be minor, having no real potential for impacting the election results or public perception of the elections process, or they could be major incidents requiring prompt action to ensure the actual or perceived integrity of the election results. An incident could be a direct attack on some portion of the election system, or it could be a potential threat that might affect confidence in the system (e.g., a reported major flaw in a foundational COTS component of many election systems).

Experience shows that successful incident response depends almost entirely on planning and preparation—the work done before any incident occurs. Good technical and process controls will minimize the attack surface and also help to enable timely analysis of the incident. Identifying key decision-makers and their roles ahead of time allows for effective response.

Planning and preparing begins with creating a plan for diagnosing and recovering from incidents and exercising this plan. To properly develop and exercise these plans, efforts must include a wide variety of stakeholders—ideally all stakeholders that would be involved in response to and recovery from the incident itself. All stakeholders, including seemingly sovereign ones such as federal, state, and local officials, must collaborate in incident response and recovery; they must also collaborate in preparing for those incidents. As the threats change, so must plans. Officials must update documentation regularly and include specific plans for addressing modern cybersecurity risks, such as those presented throughout Part 2.

In practice: recovery ready in Cook County and California

In Illinois, since 2007, the Cook County Clerk's office has worked with an independent data analysis firm, Data Defenders, LLC, which has implemented its Applied Computer Forensics process, called Election System Auditing (ESA)™, as part of an overall election integrity management plan.

For each election, the forensics process takes three "snapshots" of the election equipment: one prior to pre-election logic and accuracy testing (Pre-LAT), one immediately after Pre-LAT, and a final one after the election has finished and the equipment is returned from the polling places and early voting sites.

These snapshots capture all of the information that makes up the software and firmware. Snapshots are encrypted and hashed so that any tampering with the snapshot will be immediately detectable. The three snapshots' hash values are compared with each to see if the software has been altered at any stage of the election process.

A reference copy of all software and firmware used by the voting system is obtained by the County Clerk from a third party source such as NIST or from a certified Voting Systems Testing Laboratory. The forensic analysis compares the before and after images listed above to the reference copy and reports on any discrepancies.

The reporting identifies any altered or deleted files, programs, scripts, or other operating components. In the case of a discrepancy, the analysis can recover the information and identify the precise lines of code that were added, altered or deleted.

Not all jurisdictions take this approach. In California, for example, the state requires that a master image be created and that image be reinstalled prior to every election. The master images are created using the trusted build files that are provided to the jurisdiction by the EAC or State of California. The trusted build is the file that is built from the source code that was reviewed and certified.

The decision of how often to create master images are a case-by-case decision, but the broader point remains: the ability to restore from a backup is critical to graceful recovery, and the ability to compare a system to a known good state is critical for identifying problems.

Incident response generally follows a lifecycle of: prepare; detect and analyze; contain, eradicate, and recover; and manage post-incident. Again, it begins with documenting and exercising, but in recovery this includes specific information about the systems and processes that may be impacted, such as knowing the hardware and software comprising specific systems, as well as things such as hashes of critical files—a way to validate whether a file has been tampered with from its last known good state. In preparing for incident recovery, one of the most critical mitigation strategies is to ensure proper backups that are secured separately from the affected systems and networks in advance of a potential incident.

The process of actually recovering starts with understanding the incident. As part of that analysis, decision-makers need to understand the impact of the incident so they can prioritize resources appropriately. Recovery is about getting back to a viable state—in some cases, the priority isn't to directly fix the problem, but rather to work around it to get to the desired outcome without the affected system. This is nothing new in the elections context: when a vote capture device breaks, it may be desirable to fix it, but it may be better at the moment to move to paper ballots so votes can be cast efficiently. The same logic may apply in a cybersecurity context across the elections ecosystem; the most important reaction is often to return to an operational state, even if it's not the optimal state.

Recovery, then, is about getting to the best possible outcome in light of the current circumstances. With proper planning and exercising, officials can avoid the impact of an incident that could prevent successfully executing an election, even when seemingly all has gone wrong.

Attacks such as those that would be directed at an election come with a motivation to impact the election in some way. Nothing serves as a greater disincentive to an attacker than knowing that their target will recover quickly and completely. And little serves to build trust with the public like a plan to achieve an accurate result even if an attack is successful. Just as with other aspects of cybersecurity, by taking the time to prepare before an incident occurs, election officials can actually turn away attackers before they arrive.

Contracting for systems or services

Many organizations use contractors or vendors to provide election system components and services to support elections processes or elections system operations. Election officials should assess the contracted supply chain in addition to support provided internally. In instances where there is contract support, officials should carefully analyze requirements for security and clearly define them in the contract. The government organization that is doing the contracting has the responsibility to assess the security risks for the component or service based on an evaluation of potential threats and security weaknesses or vulnerabilities as well as the probability of occurrence and resulting consequences. Security considerations should be an important consideration in the process of evaluating and selecting a contractor.

If the elections staff is contracting for services that are managed by a contractor or vendor, such as hosting of elections-related software or operations of elections systems, the contract should require that the company providing managed services also provide documentation of their cybersecurity processes and controls, including security metrics that are being collected and monitored. Contractor controls can then be compared to the controls listed in this handbook.

The contract should include a definition of services to be delivered (called a service level agreement or SLA) that includes security controls identified in this handbook. Moreover, a best practice would be that the contractor is subjected to regular independent audits of security controls, with results available to the government organization. Elections officials may wish to have their own security audits. The contract will need to provide for this and the elections officials will need to set aside funds for the audits.

For elections system components that are subject to elections system certification requirements, evidence of certification is required. Ideally, there should also be a provision for the contractor to provide security updates to the component over its lifecycle to ensure that vulnerabilities that are discovered are corrected and the component is recertified. For system components or services that are not subject to certification, security requirements will need to align with the particular capabilities or services provided in the contract. Many of the best practices listed in this handbook may be appropriate to include as contract requirements.

In general, the contract should require that the contractor provide a security plan as one of the initial contract deliverables. The security plan should describe how the contractor will meet the security obligations of the contract and specify the security practices and procedures that will be used. Of particular importance in specifying security requirements for contractors will be to address how elections-sensitive information (e.g., ballot layout, voter personal information, vote results) is protected during the execution of the contract and how information records are destroyed.

Additionally, contracts should address the obligations of contracted system operators and public sector clients in regards to identity theft liability, control of and access to public and private data under open records laws, and incident response plans and processes. Where possible, contracts also should specify that vendors transmit network, system, and application logs to the client's security information and event management tools if the client requests. This would allow election officials and their staffs to review and monitor activity instead of being solely reliant on the vendor's capacity for monitoring.

Guidelines for ensuring security of contracted support has been described in the publication ISO/IEC 27002. Specifically, section 15 of the standard describes security issues that should be addressed in dealing with suppliers. The Appendix to this handbook contains a reproduction of this section.

Contracting and technical personnel are encouraged to use this or a similar resource to help identify and assess potential risks as well as responsibilities that will need to be addressed in contract documents and in managing suppliers.

Security best practices

These recommendations are derived from extensive experience understanding the types of vulnerabilities found and attacks experienced across a very wide variety of enterprises, and then translating that into specific and positive steps to mitigate those vulnerabilities and threats. Those recommendations are tailored based on the system and "mission" issues that are unique to elections systems, and the confidence expected for successful outcomes. The process used also examined the various guidelines and specifications used in this sector in order to maintain consistency and minimize overlap.

All of the recommended practices are grouped by class of connectedness (i.e., network connected, indirectly connected, transmission), which was identified as the key factor in assessing security risk. In addition, recommended practices that specifically deal with transmission (electronically or manually) are grouped as a collection for ease of reference.

Network Connected

Network connected components work directly with other devices or systems to achieve their objectives. These connections provide many benefits (e.g., remote diagnostics and management, simple data transfer, rapid updating), but also introduce additional risks that must be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means to accessing and managing the devices, which means organizations must take extra efforts to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet.

Indirectly Connected

Indirectly connected components are not persistently interconnected with other devices. They do, however, have to exchange information in order to complete their objectives in the election process. While these devices do not carry the same risks associated with being connected to a network or the internet, connecting these components to other devices, either through the use of removable media or direct wired connects, can introduce threats. Mitigating these risks requires a particular set of controls and recommendations when managing the device.

Transmission

In addition to the level of network connectedness, recommendations to address the broader risk of transmission of information across systems are listed separately. These can provide different and sometimes unexpected avenues of attack. These can also involve information transmitted to or from supporting systems that are easy to overlook in terms of security criticality (e.g., the printing of pollbooks, scheduling systems).

Structure of the best practices

Each best practice includes the following information:

- Asset Class (Device, Process, Software, User) — the portion of the overall system to which the practice applies.
- Priority (High, Medium, Low) — from a security perspective (in this handbook, only High and Medium practices have been included).
- Applicable CIS Controls — a cross-reference to the most applicable of the CIS Controls (which can provide a deeper description of this type of practice, and pointers to other information).

We also provide information intended to help decision-makers calibrate the potential challenges of implementation. However, these should be treated as rough guidelines for a "typical" situation – not a rule that can be applied to every election system.

- Potential User Resistance (Yes/No) — Would implementation of the practice be expected to cause resistance or complaints by users and operators of the system? If so, extra care might be needed for rollout or training; and care should be taken so that implementation doesn't encourage the use of risky "work-arounds."
- Upfront Cost (High, Medium, Low) — Does this practice typically require the purchase of new technology, or other significant capital expenditure (High)? Items can be listed as Low when no separate purchase is needed, often because the recommendation can be implemented using existing technology, into the basic configuration of the purchased system, or through operator action.
- Operational Cost (High, Medium, Low) — What are the expected post-purchase costs of this practice? Are there high costs associated with things like supplies (e.g., media, special licensing)?

Summary of connectedness in elections infrastructure components

Part 2 describes the components of a generalized elections system. The end of each subsection classified the different approaches to implementing each component based on the extent to which the component is connected to networks. These connectedness classifications are summarized in Table 1 and form the basis of the best practices. Depending on specific implementation, some of these classifications may vary. However, unless compelling information suggests otherwise, components should be protected at the level indicated.

From Part 2, election officials and others should be able to step through each component to determine the manner (or manners) in which it is implemented in a given election jurisdiction. Once the approach is known, the connectedness classification, summarized here, maps to specific sets of best practices found in the remainder of Part 3.

As noted in Part 2, the components below are a subset that, in our view, reflect the highest risk targets. For digital components not listed below, the analysis methods described in Part 2 can be applied to determine the appropriate correctness class and the associated best practices applicable to that component.

Practitioners can implement these best practices in any order, but we recommend beginning with the high priority best practices.

TABLE 1:
Summary of connectedness for elections infrastructure components

Component		Type within component	Connectedness Class
Voter registration		Master systems and databases	Network connected
	1	Online	Network connected
	2	Paper-based	Not connected
		Transmission of a registration via email or fax	Transmission-based
Pollbooks		e-Pollbook, connects via a wired or wireless network	Network connected
		e-Pollbook, connects via a physical media connection or removable media	Indirectly connected
		Transmission of data for printing via a network connection, website portal, or email	Transmission-based
		Transmission of data for printing via a wired media connection or removable media	Transmission-based
EMS	1	Unless definitively known to have no network capabilities	Network connected
	2	If known definitively to have no network capabilities	Indirectly connected
Vote capture		Vote capture device transmits data for any reason—or if the functionality is enabled regardless of whether it is used	Network connected
	1	Voter marked and hand counted paper balloting	Not connected
	2	Voter marked paper balloting with scanning	Indirectly connected
	3	Electronic voting with paper ballot output	Indirectly connected
	4	Electronic voting with paper record	Indirectly connected
	5	Electronic voting with no paper record	Indirectly connected
	6	Electronic receipt and delivery of ballots conducted remotely	Transmission-based
Vote tabulation	1	Connects via a wired or wireless connection	Network connected
	2	All others	Indirectly connected
Election night reporting	1	If receiving tabulated votes via a wired or wireless connection	Network connected
	2	If receiving tabulated votes via a wired media connection or removable media	Indirectly connected
Election night publishing	1	All	Network connected

Best Practices

The following best practices address the risks identified elsewhere in this handbook. References to resources are listed in the Appendix.

Connectedness Class	Priority
Network Connected	**High**

1 Whitelist which IPs can access the device

Applicable CIS Controls

#14: Controlled Access Based on the Need to Know
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources
CISCO recommendations on how to implement Access Control Lists on Perimeter Devices: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

2 Regularly scan the network to ensure only authorized devices are connected

Applicable CIS Controls

#1.1: Automated Asset Inventory Tool
Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

#12.8: Periodically Scan For Back-channel Connections To The Internet
Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources
Automated tools should be available to actively scan the internal environment, while DHS and MS-ISAC services can assist organizations with scanning their externally facing assets.

continued:

Connectedness Class
Network Connected

Priority
High

3 Limit the devices that are on the same subnet to only those devices required

Applicable CIS Controls

#14.1: Implement Network Segmentation Based On Information Class
Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are able to communicate with systems necessary to fulfill their specific responsibilities.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources
NIST guidance is available to help the technical team determine how to appropriately segregate assets and permit access to only those devices or systems requiring access: https://nvd.nist.gov/800-53/Rev4/control/SC-7.

4 Only utilize approved and managed USB devices with appropriate device encryption and device authentication

Applicable CIS Controls

#14: Controlled Access Based on the Need to Know
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Low

Resources
CISCO recommendations on how to implement Access Control Lists on Perimeter Devices: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

continued:

Connectedness Class
Network Connected

Priority
High

5 Disable wireless peripheral access of devices unless required and the risk is formally approved by election officials

Applicable CIS Controls

#15.8: Disable Wireless Peripheral Access (Bluetooth, WiFi, radio, microwave, satellite, etc.) Unless Required
Disable wireless peripheral access of devices (such as Bluetooth and WiFi), unless such access is required and risk acceptance is formally documented.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources
Microsoft guidance on how to disable Bluetooth: https://technet.microsoft.com/en-us/library/dd252791.aspx.

6 Ensure the system is segregated from other independent election systems and non-election supporting systems

Applicable CIS Controls

#14.1: Implement Network Segmentation Based On Information Class
Segment the network based on the type of information and the sensitivity of the information processes and stored. Use virtual LANS (VLANS) to protect and isolate information and processing with different protection requirements with firewall filtering to ensure that only authorized individuals are able to communicate with systems necessary to fulfill their specific responsibilities.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	High	Medium

Resources
While this is an often overlooked control and can require architectural redesigns, this is an important control to pursue. NIST guidance on boundary protection: https://nvd.nist.gov/800-53/Rev4/control/SC-7.

continued:

Connectedness Class
Network Connected

Priority
High

7 Deploy Network Intrusion Detection System (IDS) (e.g., MS-ISAC Albert sensor) on Internet and extranet DMZ systems

Applicable CIS Controls

#12.2: Record At Least Packet Header Information On DMZ Networks
On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources
The Albert device is part of the MS-ISAC offering: https://www.cisecurity.org/ms-isac/services/albert/. There are a number of commercially-available options, such as: https://securityonion.net/.

8 If wireless is required, ensure all wireless traffic use at least Advanced Encryption Standard (AES) encryption with at least Wi-Fi Protected Access 2 (WPA2)

Applicable CIS Controls

#15.5: Protect All Wireless Traffic with AES and WPA2
Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Low

Resources
NIST guidance on how to implement secure wireless networks: https://www.nist.gov/publications/guidelines-securing-wireless-local-area-networks-wlans.

9 Use trusted certificates for any publicly-facing website

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources
Vendor recommendation on deploying certificates with the system. Also, test to verify SSL certificate configuration, with products such as with Qualys: https://www.ssllabs.com/ssltest/.

continued:

Connectedness Class
Network Connected

Priority
High

10 Ensure logs are securely archived

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources
Work with appropriate vendors. Additionally, see Microsoft's How to Set Event Log Security: https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

11 On a regular basis, review logs to identify anomalies or abnormal events

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

12 Ensure critical data is encrypted and digitally signed

Applicable CIS Controls

#13.2: Deploy Hard Drive Encryption Software
Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources
Work with appropriate vendors. Additionally, see Microsoft guidance on digital signatures: https://technet.microsoft.com/en-us/library/cc962021.aspx.

13 Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Low	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

continued:

Connectedness Class
Network Connected

Priority
High

14 Perform system testing prior to elections (prior to any ballot delivery), such as acceptance testing

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

15 Ensure acceptance testing is done when receiving or installing new/updated software or new devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Low	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

16 Conduct criminal background checks for all staff including vendors, consultants, and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources
Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

continued:

Connectedness Class
Network Connected

Priority
High

17 Deploy application whitelisting

Applicable CIS Controls
 # 2.2: Deploy Application Whitelisting
Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Medium	Low

Resources
NIST guidance on how to implement application whitelisting: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf. May have to work with the vendors to implement it on their systems.

18 Work with election system provider to ensure base system components (e.g., OS, database) are hardened based on established industry standards

Applicable CIS Controls
#3.1: Establish Standard Secure Configurations For OS And Software
Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

#18.7: Use Standard Database Hardening Templates
For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	High	Low

Resources
CIS Benchmarks provide hardened configurations for consumer grade operating systems and applications: https://www.cisecurity.org/cis-benchmarks/. In addition, NIST provides additional recommendations for baselines https://nvd.nist.gov/800-53/Rev4/control/CM-2. Some vendor products may require tailoring to work with benchmark configured systems. Deviations from the benchmark should be documented.

continued:

Connectedness Class
Network Connected

Priority
High

19 Regularly run a SCAP-compliant vulnerability scanner

Applicable CIS Controls

#4.1: Weekly Automated Vulnerability Scanning
Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Medium

Resources
Principal cost beyond the purchase of the tool is the adjudication and remediation of the findings. SCAP validated tools can be found at: https://nvd.nist.gov/scap/validated-tools and there are a number of other commercially available tools.

20 Utilize EAC certified or equivalent software and hardware products where applicable

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Medium	Medium

Resources
Guidance from EAC about their vendor certification process: https://www.eac.gov/voting-equipment/frequently-asked-questions/.

21 Store secure baseline configuration on hardened offline system and securely deploy baseline configurations

Applicable CIS Controls

#3.3: Store Master Images Securely
Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

continued:

Connectedness Class
Network Connected

Priority
High

22 Utilize write-once media for transferring critical system files and system updates. Where it is not possible to use write-once media, that media should be used one time (for a single direction off transfer to a single destination device) and securely dispose of the media.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Low

Resources
NIST guidance on Media Protection: https://nvd.nist.gov/800-53/Rev4/control/MP-7.

23 Maintain detailed maintenance record of all system components

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Maintenance process, procedures and recommendations based on NIST guidance: https://nvd.nist.gov/800-53/Rev4/control/MA-2.

24 Require the use of multi-factor authentication

Applicable CIS Controls

#5.6: Use Multi-factor Authentication For All Administrative Access
Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards,certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

#12.6: Require Two-factor Authentication For Remote Login
Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.

#16.11: Use Multi-factor Authentication For Accounts Accessing Sensitive Data Or Systems
Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	High	Medium

Resources
Vendor specific. NIST guidance on authentication: https://pages.nist.gov/800-63-3/sp800-63b.html.

continued:

Connectedness Class
Network Connected

Priority
High

25 Require users to use strong passwords (14 character passphrases) if multi-factor authentication is not available

Applicable CIS Controls

#5.7: User Accounts Shall Use Long Passwords
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

#16.12: Use Long Passwords For All User Accounts
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Vendor specific. CIS Benchmarks details how this can be implemented for consumer grade operating systems and applications: https://www.cisecurity.org/cis-benchmarks/.

26 Limit the number of individuals with administrative access to the platform and remove default credentials

Applicable CIS Controls

#5.1: Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Connectedness Class
Network Connected

Priority
Medium

27 Ensure that all devices are documented and accounted for throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

28 Utilize tamper evident seals on all external ports that are not required for use and electronically deactivate ports where feasible

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

29 Maintain an inventory of assets that should be on the same subnet as the election system component

Applicable CIS Controls

#1.4: Asset Inventory Accounts For All Devices
Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

continued:

Connectedness Class
Network Connected

Priority
Medium

30 Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

31 Conduct load and stress tests for any transactional related systems to ensure the ability of the system to mitigate potential DDoS type attacks

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Medium	Low

32 Limit the use of personally identifiable information. When it is required, ensure that it is properly secured and staff with access are properly trained on how to handle it.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

Resources
Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

33 Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Medium	Medium

continued:

Connectedness Class
Network Connected

Priority
Medium

34 Identify and maintain information on network service providers and third-party companies contacts with a role in supporting election activities

Applicable CIS Controls
#19.5: Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

35 Implement a change freeze prior to peak election periods for major elections

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

36 Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Medium	Medium

37 Work with vendors to establish and follow hardening guidance for their applications

Applicable CIS Controls
#3.1: Establish Standard Secure Configurations For OS And Software
Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources
Vendors will typically provide recommendations on how to securely deploy and manage their systems.

continued:

Connectedness Class
Network Connected

Priority
Medium

38 Ensure logging is enabled on the system

Applicable CIS Controls

#6.2: Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Medium

Resources
Work with Vendor to identify logging capabilities. CIS-CAT can check this configuration item for consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. CIS Benchmarks provides logging recommendations for major platforms: https://www.cisecurity.org/cis-benchmarks/.

39 Use automated tools to assist in log management and where possible ensure logs are sent to a remote system

Applicable CIS Controls

#6.6: Deploy A SIEM or Log Analysis Tools For Aggregation And Correlation/Analysis
Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	High	High

Resources
A variety of tools that have various capabilities and costs as well as the effort and rigor of the review and retention of the logs which will have varying costs. Windows Event Subscription Guide: https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

continued:

Connectedness Class
Network Connected

Priority
Medium

40 Where feasible, utilize anti-malware software with centralized reporting

Applicable CIS Controls

 # 8.1: Deploy Automated Endpoint Protection Tools
Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Low

Resources
Vendor specific.

41 Ensure only required ports are open on the system through regular port scans

Applicable CIS Controls

#9.3: Perform Regular Automated Port Scanning
Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.

#9.1: Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources
Checkable by CIS-CAT and other SCAP-validated tools (https://nvd.nist.gov/scap/validated-tools), and other network scanning tools such as NMAP: https://nmap.org.

continued:

Connectedness Class
Network Connected

Priority
Medium

42 Where feasible, implement host-based firewalls or port filtering tools

Applicable CIS Controls
#9.2: Leverage Host-based Firewalls
Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Medium

Resources
If host-based, can be verified by CIS-CAT: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. Microsoft guidance on implementing firewalls: https://technet.microsoft.com/en-us/library/cc772353(v=ws.10).aspx.

43 Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7. For EAC certified voting systems, System Validation Tools are required which provide a process for validating the hash values on the system versus the trusted build (certified software).

44 Ensure vendors distribute software packages and updates using secure protocols

Applicable CIS Controls
#3.4: Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources
Work with the election software vendors.

continued:

Connectedness Class
Network Connected

Priority
Medium

45 Maintain a chain of custody for all core devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

46 All remote connections to the system will use secure protocols (TLS, IPSEC)

Applicable CIS Controls
#3.4: Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as, TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
CIS-CAT can identify whether secure protocols are configured consumer grade operating system: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. Microsoft guidance on securing remote access: https://msdn.microsoft.com/en-us/library/cc875831.aspx.

47 Users will use unique user IDs

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Individual accountability is one of the linchpins in cybersecurity and is useful for auditing events and actions taken on a system. Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

continued:

Connectedness Class
Network Connected

Priority
Medium

48 Use a dedicated machine for administrative tasks to separate day to day functions from other security critical functions. (For some components this may not be practical to implement.)

Applicable CIS Controls

#5.9: Use Dedicated Administrative Machines
Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Medium	Low

Resources
For some components this may not be practical to implement.

49 Ensure that user activity is logged and monitored for abnormal activities

Applicable CIS Controls

#16.10: Profile User Account Usage And Monitor For Anomalies
Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Medium	Medium

Resources
CIS-CAT can identify these at the consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. It is desirable to have a log aggregation or SIEM system in place to aggregate and analyze logs for abnormal behaviors.

continued:

Connectedness Class
Network Connected

Priority
Medium

50 Regularly review all accounts and disable any account that can't be associated with a process or owner

Applicable CIS Controls

#16.3: Ensure System Access Is Revoked Upon Employee/Contractor Termination
Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

51 Establish a process for revoking system access immediately upon termination of employee or contractor

Applicable CIS Controls

#16.3: Ensure System Access Is Revoked Upon Employee/Contractor Termination
Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Resources on the process potentially involved with termination process NIST: https://nvd.nist.gov/800-53/Rev4/control/PS-4.

continued:

Connectedness Class
Network Connected

Priority
Medium

52 Ensure that user credentials are encrypted or hashed on all platforms

Applicable CIS Controls

#16.14: Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
CIS-CAT can identify this configuration on consumer grade operating systems and applications, work with vendor to verify: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.

53 Ensure all workstations and user accounts are logged off after a period of inactivity

Applicable CIS Controls

#16.5: Configure screen locks on systems to limit access to unattended workstations.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Work with dedicated purpose election system vendors to verify their products. CIS-CAT can identify this configuration on consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.

54 Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Connectedness Class
Indirectly Connected

Priority
High

55 For data transfers that utilize physical transmission, utilize tamper evident seals on the exterior of the packaging

Applicable CIS Controls

#13.5: Disable Write Capabilities To USB Devices
If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	High	No	Medium	Low

Resources
Windows guidance on how to restrict hardware devices: https://technet.microsoft.com/en-us/library/cc771759(v=ws.10).aspx. Best practice is the use of specially designed USB keys that allow for encryption and device authentication.

56 Disable wireless peripheral access of devices

Applicable CIS Controls

#15.8: Disable Wireless Peripheral Access (i.e. Bluetooth) Unless Required
Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	High	No	Low	Low

Resources
Windows guidance on how to restrict hardware devices: https://technet.microsoft.com/en-us/library/cc771759(v=ws.10).aspx. Best practice is the use of specially designed USB keys that allow for encryption and device authentication.

continued:

Connectedness Class
Indirectly Connected

Priority
High

57 Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Low	Low

Resources
Work with appropriate vendors. Review EAC Guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

58 Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Medium	Medium

Resources
Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

59 Ensure staff is properly trained for reconciliation procedures for the pollbooks to the voting systems and reconcile every polling place and voter record in accordance with local, state, and federal guidelines

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Low	Low

60 Store secure baseline configurations on hardened offline systems and securely deploy baseline configurations

Applicable CIS Controls

#3.3: Store Master Images Securely
Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

continued:

Connectedness Class
Indirectly Connected

Priority
High

61 Work with the vendor to deploy application whitelisting

Applicable CIS Controls

#2.2: Deploy Application Whitelisting
Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	Yes	Medium	Low

Resources
NIST guidance on how to implement application whitelisting: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf. May have to work with the vendors to implement it on their systems.

62 Utilize the most up-to-date and certified version of vendor software

Applicable CIS Controls

#4.5: Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

#18.1: Use Only Vendor-supported Software
For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low Medium	

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

continued:

Connectedness Class
Indirectly Connected

Priority
High

63 Utilize write-once media for transferring critical system files and system updates. Where it is not possible to use write-once media, that media should be used one time (for a single direction off transfer to a single destination device) and securely dispose of the media.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low	Low

Resources
NIST guidance on Media Protection: https://nvd.nist.gov/800-53/Rev4/control/MP-7.

64 Only use the devices for election related activities

Applicable CIS Controls
#5.9: Use Dedicated Administrative Machines
Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Medium	Low

Resources
Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

65 Maintain detailed maintenance records of all system components

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	High	No	Low	Low

Resources
Maintenance process, procedures and recommendations based on NIST: https://nvd.nist.gov/800-53/Rev4/control/MA-2.

continued:

Connectedness Class
Indirectly Connected

Priority
High

66 Limit the number of individuals with administrative access to the platform and remove default credentials

Applicable CIS Controls
#5.1: Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	High	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Connectedness Class
Indirectly Connected

Priority
Medium

67 Utilize tamper evident seals on all external ports that are not required for use

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

68 Ensure that all devices are documented and accounted for throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

69 Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

70 Perform system testing prior to elections (prior to any ballot delivery), such as logic and accuracy testing

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

71 Ensure acceptance testing is done when receiving or installing new or updated software or new devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

72 Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Medium

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

73 Identify and maintain information on network service providers and third-party companies' contacts with a role in supporting election activities

Applicable CIS Controls
#19.5: Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

74 Implement a change freeze prior to peak election periods for major elections

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

75 Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Medium

76 Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	Medium	No	Medium	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7. For EAC certified voting systems, System Validation Tools are required which provide a process for validating the hash values on the system versus the trusted build (certified software).

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

77 Ensure the use of unique user IDs

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources
Individual accountability is one of the linchpins in cybersecurity and is useful for auditing events and actions taken on a system. Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

78 Ensure individuals are only given access to the devices they need for their job

Applicable CIS Controls
#14: Controlled Access Based on the Need to Know
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources
How to implement least privilege within an organization according to NIST: https://nvd.nist.gov/800-53/Rev4/control/AC-6.

79 Maintain a chain of custody for all core devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

80 Ensure all workstations and user accounts are logged off after a period of inactivity

Applicable CIS Controls
#16.5: Configure screen locks on systems to limit access to unattended workstations

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources
CIS-CAT can identify this configuration on consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.
Work with special purpose election system vendors to verify their products.

continued:

Connectedness Class
Indirectly Connected

Priority
Medium

81 Regularly review all authorized individuals and disable any account that can't be associated with a process or owner

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Medium	Medium

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

82 Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Connectedness Class
Transmission

Priority
High

83 Use secure protocols for all remote connections to the system (TLS, IPSEC)

Applicable CIS Controls
#3.4: Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that Table5 not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	High	No	Low	Low

Resources
CIS-CAT can identify whether secure protocols are configured for common operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.
Microsoft guidance on securing remote access: https://msdn.microsoft.com/en-us/library/cc875831.aspx.

continued:

Connectedness Class
Transmission

Priority
High

84 Ensure critical data is encrypted and digitally signed

Applicable CIS Controls
#13.2: Deploy Hard Drive Encryption Software
Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	High	No	Medium	Medium

Resources
Work with appropriate vendors. Additionally, see Microsoft's How to Set Event Log Security:
https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

Connectedness Class
Transmission

Priority
Medium

85 Ensure the use of bi-directional authentication to establish trust between the sender and receiver

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Medium	Low

86 For data transfers that utilize physical transmission utilize tamper evident seals on the exterior of the packaging

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their product offerings. Additionally see information on tamper evident seals:
http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

continued:

Connectedness Class
Transmission

Priority
Medium

87 Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Medium	Medium

Resources
Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

88 Track all hardware assets used for transferring data throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

Appendix: References and Resources

This section provides references to the resources cited in this handbook, including Section 15 of ISO/IEC 27002, which we reproduce with permission from ISO.

In addition, the website for this handbook, https://www.cisecurity.org/elections-resources/, has additional resources, such as more best practices from local elections officials, that may be useful for readers.

CIS resources

Under the sponsorship of the U.S. Department of Homeland Security, CIS offers a number of services to U.S. State, Local, Tribal, and Territorial (SLTT) government entities at no charge. Specifically, SLTT entities can take advantage of the following resources:

- Become members of the MS-ISAC (Multi-State Information Sharing and Analysis Center) for coordination of cybersecurity readiness and response (https://www.cisecurity.org/ms-isac/)
- Access the CIS Controls—20 foundational and advanced cybersecurity actions that can eliminate the most common attacks (https://www.cisecurity.org/controls/)
- Access the CIS Benchmarks—a set of configuration guidelines to safeguard operating systems, software, and networks (https://www.cisecurity.org/cis-benchmarks/)
- Obtain membership to CIS SecureSuite—a set of integrated cybersecurity resources to help start secure and stay secure (https://www.cisecurity.org/cis-securesuite/)
- Use CIS-CAT Pro, to quickly compare and report on the configuration of systems against CIS Benchmark recommendations (https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/)
- Purchase through CIS CyberMarket—a program to improve cybersecurity through cost-effective group procurement (https://www.cisecurity.org/services/cis-cybermarket/)
- Access CIS WorkBench—a community website that serves as a hub for tech professionals to network, collaborate, discuss technical concepts, and download CIS resources (https://www.cisecurity.org/introducing-cis-workbench/)

CIS has gathered additional resources specific to the elections community at https://www.cisecurity.org/elections-resources/. In addition to an electronic version of the handbook, the site includes additional examples of best practices in use in state and local jurisdictions, as well as other resources that may be useful to organizations implementing the best practices.

CIS also provides support beyond that funded by DHS (called "partner paid" services) if needed by SLTT organizations. Examples of partner paid services include additional Albert sensors and security monitoring services as well as tailored cybersecurity support.

Individuals working for any State, Local, Tribal, or Territorial government should contact CIS at info@msisac.org to find out what's best for their organization. Commercial entities, such as vendors of election systems and service providers, are also welcomed to access many of these services, in many cases free of charge.

Other resources referenced in this handbook

Department of Homeland Security. https://www.dhs.gov/.

Designation of chief State election official, 52 USC 20509 (2014). Accessed at https://www.gpo.gov/fdsys/pkg/USCODE-2014-title52/html/USCODE-2014-title52-subtitleII-chap205-sec20509.htm.

Election Assistance Commission. https://www.eac.gov/.

Election Assistance Commission. (2015). *Election Assistance Commission Statutory Overview: 2014.* Retrieved from https://www.eac.gov/assets/1/1/2014_Statutory_Overview_Final-2015-03-09.pdf.

Financial Sector Information Sharing and Analysis Center. https://fsisac.com/.

Harris, Joseph P. (1934). *Election Administration in the United States.* Brookings Institution Press, Washington D.C. Retrieved from https://www.nist.gov/itl/election-administration-united-states-1934-joseph-p-harris-phd.

International Organization for Standardization. (2011). *Information technology—Security techniques—Information security risk management.* ISO/IEC 27005:2011. Available at https://www.iso.org/standard/56742.html.

International Organization for Standardization. (2013). *Information technology—Security techniques—Code of practice for information security controls.* ISO/IEC 27002:2013. Available at https://www.iso.org/standard/54533.html.

National Institute of Standards and Technology. (2012). *Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments.* NIST SP800-30. Available at https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Available at https://www.nist.gov/cyberframework.

"Principles and Best Practices for Post-Election Audits." Edited by Mark Lindeman et al., Principles and Best Practices for Post-Election Audits, 1 Sept. 2008, www.electionaudits.org/principles.html.

Volunteer Voting System Guidelines, version 1.1. (2015). *Elections Assistance Commission.* Available at https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/.

Summary of resources referenced in this handbook's best practices

Cisco Systems, Inc. "Configuring IP Access Lists." *Cisco,* 5 June 2017, https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

Election Assistance Commission. "Election Management Guidelines." *U.S. Election Assistance Commission (EAC),* https://www.eac.gov/election-officials/election-management-guidelines/.

Fyodor. "Nmap." *Nmap: the Network Mapper - Free Security Scanner,* 1 Aug. 2017, https://nmap.org/.

General Services Administration. "GSA Forms Library." *Basic National Agency Check Criminal History,* 17 Aug. 2017, https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

Johnston, Roger G. "Tamper-Indicating Seals: Practices, Problems, and Standards." *World Customs Organization Security Meeting,* 11 Feb. 2003, http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

Microsoft Corp, Inc. "Digital signatures." *Microsoft TechNet,* https://technet.microsoft.com/en-us/library/cc962021.aspx.

Microsoft Corp, Inc. "Disabling Bluetooth and Infrared Beaming." *Microsoft TechNet,* 9 Feb. 2009, https://technet.microsoft.com/en-us/library/dd252791.aspx.

Microsoft Corp, Inc. "Event Subscriptions." *Windows Server 2008 R2 and Windows Server 2008,* 22 Feb. 2013, https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

Microsoft Corp, Inc. "How to Set Event Log Security Locally or by Using Group Policy." *How to Set Event Log Security Locally or by Using Group Policy,* 7 Jan. 2017, https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

Microsoft Corp, Inc. "Lesson 1: Managing User Accounts." *Microsoft Developer Network,* https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Microsoft Corp, Inc. "Managing Windows Firewall with Advanced Security." *Windows Server 2008 R2 and Windows Server 2008,* 2 July 2012, https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

Microsoft Corp, Inc. "Securing Remote Access." *Microsoft Developer Network,* https://msdn.microsoft.com/en-us/library/cc875831.aspx.

National Institute of Standards and Technology. (2012). *Special Publication 800-153: Guidelines for Securing Wireless Local Area Networks.* NIST SP 800-153. Available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf.

National Institute of Standards and Technology. (2013). *Special Publication 800-35 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations.* NIST SP 800-53r4. Available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

National Institute of Standards and Technology. (2015). *Special Publication 800-167: Guide to Application Whitelisting.* NIST SP 800-167. Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

National Institute of Standards and Technology. (2017). *Special Publication 800-63B: Digital Identity Guidelines Authentication and Lifecycle Management.* NIST SP 800-63B. Available at https://pages.nist.gov/800-63-3/sp800-63b.html.

National Institute of Standards and Technology. *National Vulnerability Database.* Available at https://nvd.nist.gov.

Onion Solutions, LLC. "Security Onion." *Security Onion,* https://securityonion.net/.

Qualys, Inc. "SSL Server Test." *SSL Server Test,* (2018), https://www.ssllabs.com/ssltest/.

ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls

©ISO. This material is reproduced from ISO/IEC 27002:2013 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

15 Supplier relationships
15.1 Information security in supplier relationships
15.1.1 Information security policy for supplier relationships

Control
Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

Implementation guidance
The organization should identify and mandate information security controls to specifically address supplier access to the organization's information in a policy. These controls should address processes and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement, including:

a) identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information;
b) a standardised process and lifecycle for managing supplier relationships;
c) defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;

d) minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and requirements and its risk profile;
e) processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;
f) accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;
g) types of obligations applicable to suppliers to protect the organization's information;
h) handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers;
i) resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;
j) awareness training for the organization's personnel involved in acquisitions regarding applicable policies, processes and procedures;
k) awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;
l) conditions under which information security requirements and controls will be documented in an agreement signed by both parties;
m) managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

Other information
Information can be put at risk by suppliers with inadequate information security management. Controls should be identified and applied to administer supplier access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements can be used. Another example is data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

15.1.2 Addressing security within supplier agreements

Control
All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Implementation guidance
Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfill relevant information security requirements.

The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information;
b) classification of information according to the organization's classification scheme (see 8.2); if necessary also mapping between the organization's own classification scheme and the classification scheme of the supplier;

c) legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;
d) obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;
e) rules of acceptable use of information, including unacceptable use if necessary;
f) either explicit list of supplier personnel authorized to access or receive the organization's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel;
g) information security policies relevant to the specific contract;
h) incident management requirements and procedures (especially notification and collaboration during incident remediation);
i) training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures; relevant regulations for sub-contracting, including the controls that need to be implemented;
j) relevant agreement partners, including a contact person for information security issues;
k) screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;
l) right to audit the supplier processes and controls related to the agreement;
m) defect resolution and conflict resolution processes;
n) supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;
o) supplier's obligations to comply with the organization's security requirements.

Other information
The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant information security risks and requirements. Supplier agreements may also involve other parties (e.g. sub-suppliers). The procedures for continuing processing in the event that the supplier becomes unable to supply its products or services need to be considered in the agreement to avoid any delay in arranging replacement products or services.

15.1.3 Information and communication technology supply chain

Control
Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Implementation guidance
The following topics should be considered for inclusion in supplier agreements concerning supply chain security:

a) defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;
b) for information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;
c) for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain
d) if these products include components purchased from other suppliers;

e) implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;
f) implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside
g) of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;
h) obtaining assurance that critical components and their origin can be traced throughout the supply chain; obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;
i) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;
j) implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

Other information
The specific information and communication technology supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organizations are advised to work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided. Organizations can influence information and communication technology supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the information and communication technology supply chain.

Information and communication technology supply chain as addressed here includes cloud computing services.

15.2 Supplier service delivery management

15.2.1 Monitoring and review of supplier services

Control
Organizations should regularly monitor, review and audit supplier service delivery.

Implementation guidance
Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

This should involve a service management relationship process between the organization and the supplier to:

a) monitor service performance levels to verify adherence to the agreements;
b) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;
c) conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;
d) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

e) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;
f) resolve and manage any identified problems;
g) review information security aspects of the supplier's relationships with its own suppliers;
h) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see Clause 17).

The responsibility for managing supplier relationships should be assigned to a designated individual or service management team. In addition, the organization should ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. The organization should retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

15.2.2 Managing changes to supplier services

Control
Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and reassessment of risks.

Implementation guidance
The following aspects should be taken into consideration:

a) changes to supplier agreements;
b) changes made by the organization to implement:
   1) enhancements to the current services offered;
   2) development of any new applications and systems;
   3) modifications or updates of the organization's policies and procedures;
   4) new or changed controls to resolve information security incidents and to improve security;
c) changes in supplier services to implement:
   1) changes and enhancement to networks;
   2) use of new technologies;
   3) adoption of new products or newer versions/releases;
   4) new development tools and environments;
   5) changes to physical location of service facilities;
   6) change of suppliers;
   7) sub-contracting to another supplier.

Department of Homeland Security (DHS) Multi-State Information Sharing and Analysis Center (MS-ISAC)

ISAC Pilot for Election Infrastructure

October 2017

Homeland Security

ISAC PILOT
for Election Infrastructure

MS-ISAC
Multi-State Information Sharing & Analysis Center

Project Team Members

DHS
- Rob Gatlin, Program Manager
- Donna Beach, ISAC Pilot Leader for Elections Infrastructure

COLORADO
- Judd Choate, State Election Director
- Trevor Timmons, CIO
  - Hilary Rudy, Deputy Director of Elections Division
  - Rich Schliep, CISO

INDIANA
- Connie Lawson, Secretary of State
  - Brandon Clifton, Deputy Secretary of State
- Thomas Vessely, Director of IT
- Patrick Glover, Assistant Director of IT
  - Jerry Bonnet, General Counsel

NEW JERSEY
- Robert Giles, Director, Division of Elections
- Kevin Kearns, Bureau Chief, Cybersecurity Governance, Risk, and Compliance
- James Simmons, Vice President, Technology & Operations
  - Vasiliy Bessonov
  - Michael DiSimoni
  - Michael Geraghty

MS-ISAC
- Ben Spear, MS-ISAC Project Leader
- Kateri Gill, MS-ISAC Stakeholder Engagement

TEXAS
- Keith Ingram, Elections Division Director
- Scott Brandt, IT Division Director
- Marlin Craig, Information Security Officer
- Michael Winn, Travis County Director of Elections

UTAH
- Justin Lee, Director of Elections
- Mark Mitchell, IT Director
- Phil Bates, State Information Security Director
- Ricky Hatch, Weber County Clerk/Auditor
- Matt Mortensen, Weber County IT Security Specialist

VIRGINIA
- Edgardo Cortes, Elections Commissioner
- Matt Davis, CIO
- Michael Watson, CISO
  - Elizabeth Howard, Elections Deputy Commissioner

WASHINGTON
- Lori Augino, Director of Elections
- Michael Huntley, CIO
- Harold Stoehr, CISO

Homeland Security

Project Progress

Oct 12	• Initiated HSA Monthly Update
Oct 18	• Initiated Newsletter Distribution
Oct 27	• Initiated Election Specific Cyber Alerts
Oct 31	• Initiated MS-ISAC Monthly Member Call
Nov 3	• Initiated National Webcast • Initiated Vulnerability Management Profiles
Nov 9	• Initiated Monthly Situational Awareness Report
Nov 13	• Initiated Alerting of IPs and Domains
Nov 20	• Initiated Weekly Elections Cyber News Alert
Nov 21	• Onboarding Complete

Homeland Security

Operational Updates

MS-ISAC
Multi-State Information
Sharing & Analysis Center

Weekly Elections Cyber News Alert

- Purpose: Weekly news summary of open-source reporting on election cybersecurity risks and best practices.
- Design
  - Title – Source – Date
  - Summary
  - Analysis
  - Source Link
- Topics
  - Cybersecurity risk landscape for Elections Infrastructure
  - Legislative action
  - Best practices
  - General technology/cybersecurity awareness with elections link/impact
- Feedback

Homeland Security

Operational Updates

Elections Cyber Alert Modifications

- Rearranged Sections
  - Executive Overview
  - User Recommendations
  - Technical Description
  - Technical Indicators
  - Technical Recommendations

Albert Monitoring

- Existing Albert Sensors:
  - Utah
  - Virginia
- Albert sensor Deployment:
  - Colorado
  - Indiana
  - New Jersey
  - Texas
  - Washington

Homeland Security

Operational Updates

Separation of Technical and Election-Specific Alerts

- Milestone Date: Q2 2018
- Option to receive only products of your choice
  - Advisories
  - Cyber Alerts
  - Election-Specific Cyber Alerts
  - Intel Products
  - Situational Awareness Report
  - Email Notifications

Feedback Survey

- Evaluates objectives and success criteria
  - Customer Service
  - Overall Membership
  - Products and Services provided

- Tool to measure the progress and satisfaction over the course of the pilot
- Frequency: 50, 80 and 110 days

Homeland Security

Pilot Duration

60 Day Deliverables

- Election-specific products
  - Election-specific Cyber Alerts
  - Weekly Cyber News
- Traditional MS-ISAC products
  - Advisories
  - Weekly Malicious IPs and Domains
  - Situational Awareness Report
  - HSA Cyber Monthly Update
  - Newsletter
  - MS-ISAC Monthly Member Call
  - Vulnerability Management Program (VMP) Report
- Information Sharing Tools
  - Machine-to-Machine Cyber Indicator Sharing
  - HSIN Portal Access
- Albert Deployment
  - Albert sensors ordered for pilot states
  - Albert notification forwarding for states with existing sensors
- Formalized notification process

Homeland Security

Pilot Duration

90 Day Deliverables

- Election-specific products
  - Monthly Analyst-to-Analyst Exchange
  - Distribution extended to registered Elections community (20 states)
- Traditional MS-ISAC products
  - Intelligence products
- Albert deployment
  - Albert sensor delivery

120 Day Deliverables

- Election-specific products
  - Outline - Elections Fusion Analysis Report
- Albert deployment
  - Albert sensors online
  - Albert notifications

Services by Request

- Computer Emergency Response Team (CERT)
- Malicious Code Analysis Platform (MCAP)

Homeland Security

Project Communications

Email DHS SLTT Project Team at:
SLTTCyber@HQ.DHS.GOV

Homeland Security

Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC)

Common Cyber Security Language

August 2018

Common Cyber Security Language

Term	Definition
Access	The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.
Accessibility	Information is available and easily usable (formatted for convenient and immediate use).
Accuracy	The closeness between an estimated result and the (unknown) true value.
Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.
Automatic Train Protection (ATP)	A wayside and/or on-board train system to apply emergency brakes if a signal is missed by the train operator.
Automatic Train Supervision (ATS)	Provides advanced functionalities of train control, typically including advanced automatic routing and automatic train regulation.
Black-box	A device that records information, which cannot be changed or manipulated in any manner. The information recorded is used for forensic purposes. It is used in the same sense of an aviation flight recorder.
CJIS Security Policy	The Criminal Justice Information Services (CJIS) Security Policy provides appropriate controls to protect the full lifecycle of Criminal Justice Information (CJI), whether at rest or in transit. The policy also provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI.
Coherence	The degree to which data that are derived from different sources or methods, but which refer to the same phenomenon, which are similar.
Commercial-off-the-Shelf (COTS)	Products that are readily available commercially and may be used “as is.”
Communications-based Train Control (CBTC)	A continuous, automatic train control system that relies on wayside data communications and/or GPS for position sensing and uses the “moving block” principle for safe train separation rather than fixed blocks with track circuits.
Comparability	The degree to which data can be compared over time and domain.
Configuration Management	A practice and process of handling hardware, software and firmware changes systematically so that a device or system maintains its integrity over time.
Consequence	The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts along with economic impacts both direct and indirect and other negative outcomes to society.
Countermeasure	Action, measure, or device intended to reduce an identified risk.
Critical infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Critical Infrastructure Owners and Operators	Those entities responsible for day-to-day operation and investment of a particular-lar critical infrastructure entity. (Source: Adapted from the 2009 NIPP).
Critical Infrastructure Partner	Governmental entities, public and private sector owners and opera-tors and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share responsibility for securing and strengthening the resilience of the Nation’s critical infrastructure.
Criticality	Importance to a mission or function, or continuity of operations.
Cryptography	A way to encode (hide) information such that the sender intends that only the recipient should understand the message.
Cyber Incident	An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.
Cyber System	Any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services; examples include business systems, control systems, and access control systems.

Cybersecurity	The full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.
Cybersecurity (USCG-Specific)	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Cyberspace	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.
Cyclic Redundancy Check (CRC)	An error detection code used in digital networks to detect accidental changes in data during transmission or storage.
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Deterrent	Measure that discourages, complicates, or delays an adversary's action or occurrence by instilling fear, doubt, or anxiety.
Electronic Security Perimeter (ESP)	Adapted from NERC-CIP electric power regulations, a logical perimeter drawn around electronic assets in a security zone to separate it from other zones.
Emergency Cutoff (blue light) system	A safety system installed at passenger stations that cuts off traction power and notifies the control center that power has been cut at this location.
Enterprise Risk Management	Comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.
Enterprise Zone	The zone of a transit agency that handles its routine internal business processes and other non-operational; non-fire, life-safety; and non-safety-critical information.
Evaluation	Process of examining, measuring and/or judging how well an entity, procedure, or action has met or is meeting stated objectives.
Executive Order 13636	Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity frame-work; and promote and incentivize the adoption of strong cybersecurity practices.
Fail-safe	A device that fails in a manner that protects the safety of personnel and equipment.
FedRAMP	The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Fiber-optic Strand	A portion of a cable in a fiber-optic network. Each strand carries information unique to it and is isolated from all the other strands.
Fire Life-Safety Security Zone (FLSZ)	A zone containing systems whose primary function is to warn, protect or inform in an emergency. It contains systems such as fire alarms and emergency ventilation.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Human-machine Interface (HMI)	The control interface between humans and machines.
Incident	An occurrence, caused by either human action or natural phenomenon, that may cause harm and require action, which can include major disasters, emergencies, terrorist attacks, terrorist threats, wild and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, cyber attacks, cyber failure/accident, and other occurrences requiring an emergency response.
Information sharing	The process through which information is provided by one entity to one or more other entities to facilitate decision-making under conditions of uncertainty.
Inputs	Resources invested into the program or activity being measured, such as funds, employee-hours, or raw materials.

Interdependency	Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions.
Intrusion	An unauthorized act of bypassing the security mechanisms of a network or information system.
IPSec	A suite of protocols for securing Internet Protocol communications that authenticates and encrypts each IP packet in a communication session.
ISO 27001	A standard created by the International Standards Organization (ISO) to "provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)".
Loss of control	Sharing with inappropriate entities (i.e., unauthorized users) and sharing for inappropriate purposes (i.e., unauthorized uses).
Malware	Short for malicious software. Software created and used by people, usually with bad intentions to disrupt computer operations or obtain, without consent, confidential information.
Man-in-the-middle (MitM)	A type of cyber-attack where an interloper inserts him- or herself in-between two communicating devices, without either side being aware of the interloper.
Mitigation	Capabilities necessary to reduce loss of life and property by lessening the impact of disasters.
National Cyber Investigative Joint Task Force	The multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from Federal agencies, including DHS, and from State, local, and international law enforcement partners.
National Cybersecurity and Communications Integration Center	The national cyber critical infrastructure center, as designated by the Secretary of Homeland Security, which secures Federal civilian agencies in cyberspace; provides support and expertise to private sector partners and SLTT entities; coordinates with international partners; and coordinates the Federal Government mitigation and recovery efforts for significant cyber and communications incidents.
Network Resilience	The ability of a network to: (1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged); (2) recover effectively if failure does occur; and (3) scale to meet rapid or unpredictable demands.
Operationally Critical Security Zone (OCSZ)	A security zone containing systems necessary for proper operation of rail transit, such as SCADA, dispatch and ATS.
Operations Control Center	A central location that monitors, and in some cases controls, some portion of a transportation system. It may handle just one system or many systems simultaneously.
Outcomes	Events, occurrences or changes in condition that indicate programmatic progress, brought about at least in part through outputs.
Outputs	Completed or delivered products or services generated through inputs.
Patch Management	A regular, coordinated method for equipment vendors to update software and firmware fixes for their digital equipment at transit agencies in a timely and responsible manner.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, etc.
Performance management	The use of performance information to affect programs, policies, or any other organization actions aimed at maximizing the benefits of public services.
Performance measurement	Regular measurement of the results (outcomes) and efficiency of services or programs.
PIV-I	PIV Interoperable (PIV-I) cards are smartcards issued by Non-Federal Issuers that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Department or Agency.
Prevention	Those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism.
Processes	The steps that turn inputs into outputs.
Programmable Logic Controller (PLC)	An industrial computer used for automation of mechanical processes.

Recommended Practice	An APTA Recommended Practice represents a common viewpoint of those parties concerned with its provisions. The application of a Recommended Practice is voluntary.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Recovery	Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources.
Recovery	The activities after an incident to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.
Redundancy	Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.
Regional	Entities and interests spanning geographic areas ranging from large multi-State areas to metropolitan areas and varying by organizational structure and key initiatives, yet fostering engagement and collaboration between critical infrastructure owners and operators, government, and other key stakeholders within the given location.
Relevance	The degree to which the product meets user needs for both coverage and content.
Residual Risk	Risk that remains after risk management measures have been implemented.
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
Risk	The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.
Risk Assessment	Product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.
Risk Avoidance	Strategies or measures taken that effectively remove exposure to a risk.
Risk Communication	Exchange of information with the goal of improving risk understanding, affecting risk perception, and/or equipping people or groups to act appropriately in response to an identified risk.
Risk Management	The process of identifying, assessing, and responding to risk.
Risk Management	The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.
Safety Critical Security Zone	The zone that contains vital signaling, interlocking and ATP within rail transit.
Safety Critical Security Zone (SCSZ)	The zone that contains vital signaling, interlocking and ATP within rail transit.
SCADA	A control system involving a master terminal unit and remote terminal units, used for supervisory control and data acquisition.
Secure Hash Algorithm (SHA):	A family of cryptographic hash functions used to calculate a unique sum for a digital file to be used to check for later file modifications.
SSAE 16	Statement on Standards for Attestation Engagements (SSAE) 16 reporting can help service organizations comply with Sarbanes Oxley's requirement to show effective internal controls covering financial reporting.
SSI	Sensitive Security Information (SSI) is a specific category of sensitive but unclassified (SBU) information that is governed by Federal law. SSI is information obtained or developed which, if released publicly, would be detrimental to transportation security. At TSA, the goal is to release as much information as possible publicly without compromising security.
STRIDE	Defines a Microsoft method to classify computer security threats. The acronym stands for Spoofing of an id, Tampering with data, Repudiation, Information disclosure (breach), Denial of service, and Elevation of privilege.
System	Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.
Threat	A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Timeliness	Information is current (it should be released as close as possible to the period to which the information refers).
Track Circuit	An electrical circuit designed to indicate the presence or absence of a train in a specific section of track.
Transportation Security Incident	A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. In this paragraph, the term "economic disruption" does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employee-employer dispute.
Trusted (network)	Network of an organization that is within the organization's ability to control or manage. Further, it is known that the network's integrity is intact and that no intruder is present.
Unauthorized Access	Any access to an information system or network that violates the owner or operator's stated security policy.
Uncertainty	The state of being not known, indeterminate, questionable, variable.
Vector (for cyber-attack)	The path an attacker takes to attack a network.
Virtual Private Network	A computer network in which some of the connections are virtual circuits instead of direct connections via physical wires within some larger network, such as the internet.
Vital Signaling	The portion of a railway signaling network that contains vital equipment.
Vital-programmable Logic Controller (vital-PLC)	A PLC with fail-safe functions intended for safety-critical signaling and interlocking applications in rail transit.
Vulnerability	A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
White-listing	Describes a list or register of entities that are granted certain privileges, services, mobility, access or recognition.
Wi-Fi	In the broadest sense, all short-range communications that use some type of electromagnetic spectrum to send and/or receive information without wires.

A Note on the Common Cyber Language: The resources on this page have been submitted by the Common Language Initiative Team, a subcommittee of the Transportation Systems Sector Cyber Working Group (TSSCWG). While they represent a small fraction of the available documents and tools available to the Transportation Systems Sector, and the Cyber Security Community as a whole, they stand out to the individuals/modes of transportation that submitted them. Over time, this living document will be revisited to add/remove terminology and/or references to ensure its relevance. For questions or recommendations on the Common Language, please email CyberSecurity@tsa.dhs.gov.

Additional Resources

Website/Document Name	Cyber Security Language Resources
2013-2023 Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy	**http://trbcybersecurity.erau.edu/files/Transportation-Standards-Plan.pdf**
American Institute of Certified Public Accountants (AICPA)	http://ssae16.com/SSAE16_overview.html
Committee on National Security Systems- CNSS Instruction No. 4009- National Information Assurance (IA) Glossary	http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf
Cyber Risk and Insurance Forum (CRIF) Cyber Security Glossary	http://www.cyberriskinsuranceforum.com/content/cyber-security-glossary
Federal Bureau of Investigation (FBI)	https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center
Federal CIO Council	https://cio.gov/wp-content/uploads/downloads/2012/09/PIV_Interoperabillity_Non-Federal_Issuers_May-2009.pdf
General Services Administration (GSA)	http://www.fedramp.gov/
Glossary- McAfee for Consumer	http://home.mcafee.com/virusinfo/glossary?ctst=1#A
Glossary of Key Information Security Terms	http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
Glossary- Symantec Enterprise	http://www.symantec.com/security_response/glossary/
Honeywell Industrial Cyber Security Glossary	https://www.honeywellprocess.com/en-US/online_campaigns/IndustrialCyberSecurity/Pages/glossary.html
International Standards Organization (ISO)	http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
ISACA- Cybersecurity Fundamentals Glossary	http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf
Joint Publication 3-12®- Cyberspace Operations	http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)- Cyber Definitions	https://ccdcoe.org/cyber-definitions.html

NICCS- A Glossary of Common Cybersecurity Terminology	http://niccs.us-cert.gov/glossary
NIPP 2013- Partnering for Critical Infrastructure Security and Resilience	http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf
NIST- Framework for Improving Critical Infrastructure Cybersecurity	http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
PCI Security Standards Council	https://www.pcisecuritystandards.org/security_standards/
Presidential Policy Directive- Critical Infrastructure Security and Resilience (PPD-21)	https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
Presidential Policy Directive- National Preparedness (PPD-8)	http://www.dhs.gov/presidential-policy-directive-8-national-preparedness
Radio Technical Commission for Aeronautics (RTCA)- SC-216 Aeronautical Systems Security	http://www.rtca.org/content.asp?pl=108&sl=33&contentid=82
Risk Steering Committee- DHS Risk Lexicon	http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf
Roadmap to Secure Control Systems in the Transportation Sector	https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/TransportationRoadmap20120831.pdf
SANS- Glossary of Security Terms	https://www.sans.org/security-resources/glossary-of-terms/
The University of Texas at Austin- Cyber Security Glossary Terms	http://www.utexas.edu/its/glossary/secure
The University of Texas at Austin- Identity and Cybersecurity Terms	https://identity.utexas.edu/everyone/glossary-of-identity-and-cybersecurity-terms
Transportation Security Administration	https://www.tsa.gov/sites/default/files/assets/pdf/ssi/ssi_reg_5-18-04.pdf
United States Coast Guard Cyber Strategy	https://homeport.uscg.mil/cgi-bin/st/portal/uscg_docs/MyCG/Editorial/20150706/CG_Cyber_Strategy_Final.pdf?id=0f151e6b1eb70b5aa8e5776e0e07d0c2c353f8e4&user_id=087c7ada72ee5d101ec55060bf4af6ce

Online Communities

Organization	Website
NIEM- National Information Exchange Model <REGISTRATION REQUIRED>	**https://www.niem.gov/communities/emc/Pages/emerging-communities.aspx**
NIEM- National Information Exchange Model	https://www.niem.gov/communities/emc/cyber/Pages/about-cyber.aspx

Election Assistance Commission (EAC)

Glossary of Common Cybersecurity Terms

August 2018

Glossary
Common Cybersecurity Terminology

Access
Ability to make use of any information system (IS) resource.

Source: CNSSI 4009-2015

Access control
The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Source: FIPS 201-2

Access control mechanism
Security safeguards designed to detect and deny unauthorized access and permit authorized access to an information system.

Source: CNSSI 4009-2015

Advanced Persistent Threat
An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Source: NIST SP 800-39

Adversary
Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Source: NIST SP 800-30 Rev. 1 (DHS Risk Lexicon)

Air gap
An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e. data is transferred through the interface only manually, under human control).

Source: CNSSI 4009-2015

Alert
Notification that a specific attack has been directed at an organization's information systems.

Source: CNSSI 4009

Antivirus software
A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

Source: NIST SP 800-94, NIST SP 800-83 Rev. 1

Asset
A major application, general support system, high impact program, physical plan, mission critical system, personnel, equipment, or a logically related group of systems.

Source: CNSSI 4009-2015

Attack
An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.

Source: NIST SP 800-82 Rev. 2 (CNSSI 4009)

Attack signature
A specific sequence of events indicative of an unauthorized access attempt.

Source: NIST SP 800-12

Attacker
A party who acts with malicious intent to compromise an information system.

Source: NIST SP 800- 63 Rev 2

Audit
Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Source: NIST SP 800-32 (CNSSI 4009)

Audit Log

A chronological record of information system activities, including records of system accesses and operations performed in a given period.

Source: NIST SP 800-53 Rev. 4

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Source: CNSSI 4009 (FIPS 200, NIST SP 800-27 Rev. A)

Authority

The aggregate of people, procedures, documentation, hardware, and/or software necessary to authorize and enable security-relevant functions.

Source: NIST SP 800-57 Part 2

Availability
Timely, reliable access to data and information services for authorized users.

Source: CNSSI 4009-2015, NIST SP 800-70 Rev 2

Backups
A copy of files and programs made to facilitate recovery if necessary.

Source: NIST SP 800-34 Rev. 1

Black-box testing
A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as basic testing.

Source: CNSSI 4009-2015, IST SP 800-53A Rev 4. (adapted)

Blacklist
A list of entities that are blocked or denied privileges or access.

Source: CNSSI 4009-2015 (NIST SP 800-94)

Breach
Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected information.

Source: ISO/IEC 27040

(adapted)

Common Vulnerabilities and Exposures (CVE)
A nomenclature and dictionary of security-related software flaws.

Source: CNSSI-4009-2015 (NIST SP 800-126 Rev. 2)

Compromise
A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information has occurred.

Source: CNSSI-4009-2015

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Source: CNSSI 4009-2015, NIST SP 800-39

Continuous Monitoring

Maintaining ongoing awareness to support organization risk decisions.

Source: CNSSI 4009-2015 (NIST SP 800-137)

Critical infrastructure

System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Source(s): NIST SP 800-30

Critical infrastructure Sector

A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society.

Source: NIPP 2013 Partnering for Critical Infrastructure Security and Resilience

Cryptography

The use of mathematical techniques to provide security services such as confidentiality, data integrity, entity authentication, and data origin authentication.

Source: NIST SP 800-130

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Source: CNSSI 4009-2015 (NSPD-54/HSPD-23)

Data Loss

The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Source: CNSSI 4009-2015 (NIST SP 800-37)

Decipher

Convert enciphered text to plain text by means of a cryptographic system.

Source: CNSSI 4009-2015

Decryption

The process of changing ciphertext into plain text using a cryptographic algorithm and key.

Source: NIST SP 800-133

Denial of Service

The prevention of authorized access to resources or the delating of time-critical operations.

Source: NIST SP 800-33

Digital Forensics

The application of science to the identification, collection, examination, and analysis, of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

Source: NIST SP 800-86

Digital Signature

The result of a cryptographic transformation of data which, when properly implemented, provides the services of: 1) origin authentication, 2) data integrity, and 3) signer non-repudiation.

Source: FIPS 140-2

Disruption

An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Source: NIST SP 800-34 Rev. 1

Encrypt

Cryptographically transform data to produce cipher text.

Source: CNSSI 4009-2015

Encryption

The process of changing plain text into ciphertext for the purpose of security or privacy.

Source: NIST SP 800-21 Second Edition (NIST SP 800-57)

Endpoint Protection Platform

Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, antiadware, personal firewalls, host-based intrusion detection and prevention systems, etc.).

Source: NIST SP 800-128

Event

Any observable occurrence in a network or system.

Source: CNSSI 4009-2015 (NIST SP 800-61 Rev. 2)

Exfiltration

The unauthorized transfer of information from an information system.

Source: CNSSI 4009-2015 (NIST SP 800-53 Rev. 4)

Exploit

A technique to breach the security of a network or information system in violation of security policy.

Source: ISO/IEC 27039 (adapted)

Firewall

The process integrated with a computer operating system that detects and prevents undesirable applications and remote users from accessing or performing operations on a secure computer.

Source: NIST SP 800-130

Hack

Unauthorized attempt or access to an information system.

Source: CNSSI 4009-2015 (Adapted from "Hacker")

Hacker

Unauthorized user who attempts to or gains access to an information system.

Source: CNSSI 4009-2015

Hash Function

An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message, and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message.

Source: NIST SP 800-152

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Source: FIPS 200

Incident Handling

The mitigation of violations of security policies and recommended practices.

CNSSI 4009-2015, NIST SP 800-61 Rev. 2

Incident Response Plan

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems(s).

Source: CNSSI 4009-2015 (NIST SP 800-34 Rev. 1)

Indicator

A sign that an incident may have occurred or may be currently occurring.

Source: NIST SP 800-61 Rev. 2

Information Operations (I/O)

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO.

Source: CNSSI 4009-2015

Information security policy

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Source: NIST SP 800-128 (CNSSI 4009)

Information system resilience

The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

Source: CNSSI 4009-2015 (NIST SP 800-39)

Information technology

Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes computers, ancillary equipment, software, firmware, similar procedures, services, and related resources.

Source: NIST SP 800-64 Rev. 2

Insider threat

An entity with authorized access (i.e., within the security) that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Source: NIST SP 800-53 Rev. 4 (CNSSI 4009)

Interoperability

A measure of the ability of one set of entities to physically connect to and logically communicate with another set of entities.

Source: NIST SP 800-130

Intrusion

A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Source: CNSSI 4009-2015 (IETF RFC 4949 Ver 2)

Intrusion Detection and Prevention

The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents.

Source: NIST 800-94

Malware

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

Source: NIST SP 800-111

Multifactor Authentication

Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Source: NIST SP 800-53 Rev. 4

Non-repudiation

Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.

Source: NIST SP 800-32

Outside Threat

An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.

Source: NIST SP 800-32

Password

A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Source: FIPS 140-2

Patch

An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Source: NIST SP 800-123

Penetration Testing

Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Source: NIST SP 800-115

Phishing

Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Source: SP 800-45 Ver 2

Port

The entry or exit point from a computer for connecting communications or peripheral devices.

Source: NIST SP 800-82 Rev. 2

Port scanning

Using a program to remotely determine which ports on a system are open (e.g., whether the systems allow connections through those ports).

Source: NIST SP 800-82 Rev. 2 (NIST SP 800-61)

Private key

A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm. For digital signatures, the private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key.

Source: FIPS 186-4

Probe

A technique that attempts to access a system to learn something about the system.

Source: CNSSI-4009

Public key

A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm and is associated with a private key. The public key is associated with an owner and may be made public. In the case of digital signatures, the public key is used to verify a digital signature that was signed using the corresponding private key.

Source: FIPS 186-4

Quarantine

To store files containing malware in isolation for future disinfection or examination.

Source: NIST SP 800-114

Resilience

The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

Source: NIST SP 800-137 (Adapted from NIST SP 800-39)

Risk analysis

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

NIST SP 800-33

Risk assessment

The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

NIST SP 800-33

Scanning

Sending packets or requests to another system to gain information to be used in a subsequent attack.

Source: CNSSI 4009-2015

Spear Phishing

A colloquial term that can be used to describe any highly targeted phishing attack.

Source: CNSSI 4009-2015

Spoofing

Faking the sending address of a transmission to gain illegal entry into a secure system.

Source: CNSSI 4009-2015

Structured Query Language (SQL) injection

An attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code.

Source: US-CERT SQL Injection Publication

Supplier

Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain. Includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) vendors; and (iii) product resellers.

Source: NIST SP 800-161 (Adapted from ISO/IEC 15288, NIST SP 800-53 Rev. 4)

Supply Chain

A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

Source: CNSSI 4009-2015

System Integrity

The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Source: CNSSI 4009-2015 (NIST SP 800-27 Rev. A)

Tabletop Exercise

A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Source: NIST SP 800-84

Target of Attack

An information technology product or system and associated administrator and user guidance documentation that is the subject of an attack.

Source: FIPS 140-2 (Adapted from Target of Evaluation)

Threat

Any circumstance or event with the potential to adversely impact organizational operations, (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Source: CNSSI 4009-2015 (NIST SP 800-31 Rev. 1)

Trojan horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Source: CNSSI 4009-2015

Unauthorized access

Any access that violates the stated security policy.

Source: CNSSI 4009

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Source: FIPS 200 (Adapted from CNSSI 4009-2015)

Whitelist

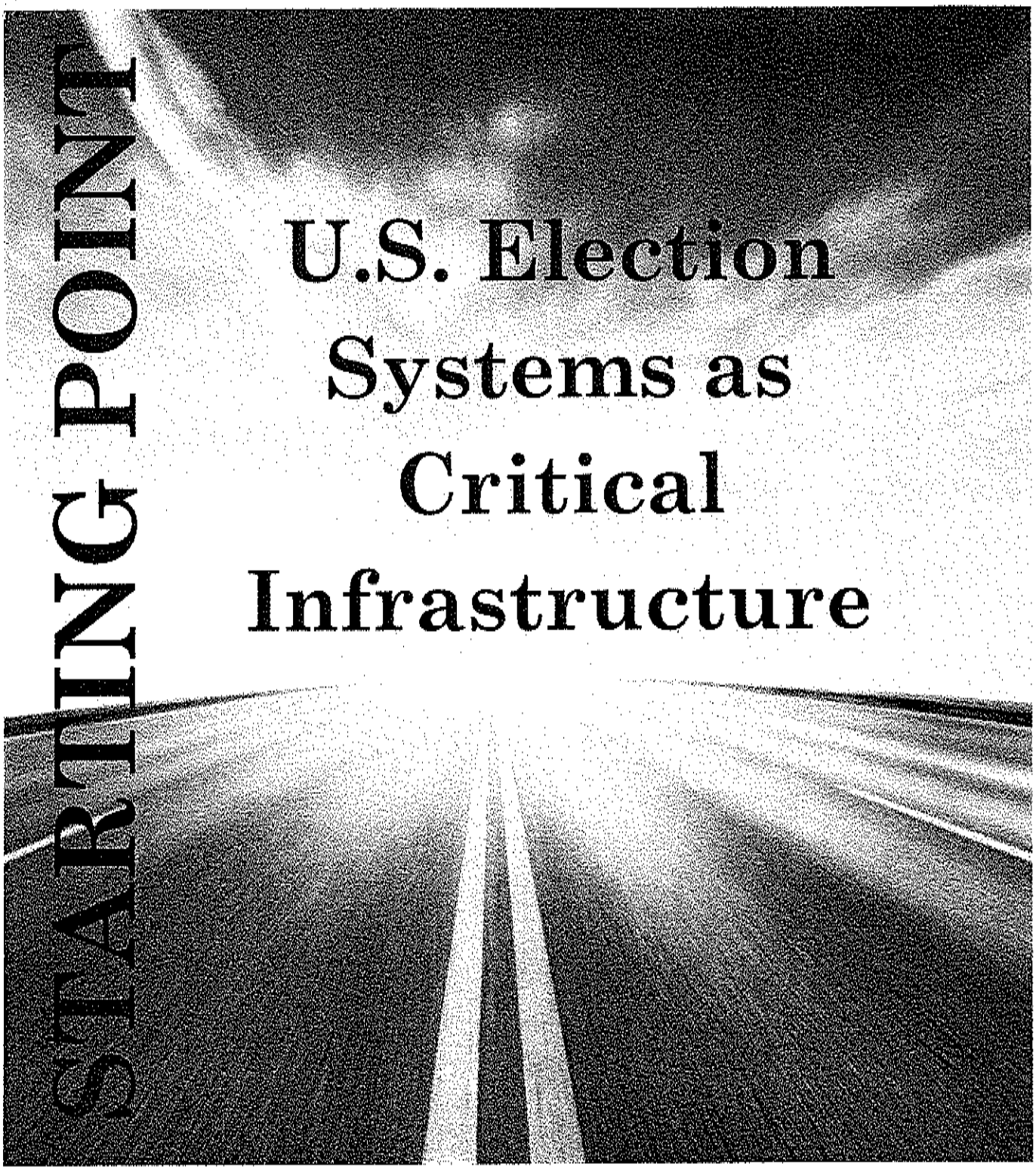
A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline.

Source: NIST SP 800-167

Election Assistance Commission (EAC)

U.S. Election Systems as Critical Infrastructure Addendum I: Glossary of Key Terms and Acronyms

February 2017



STARTING POINT

U.S. Election Systems as Critical Infrastructure

U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

12

Starting Point:

U.S. Election Systems as Critical Infrastructure

On January 6, 2017, Department of Homeland Security (DHS) Secretary Jeh Johnson designated U.S. election systems as part of the nation's critical infrastructure, a decision that was later affirmed by current DHS Secretary John Kelly. Since the designation was announced, state and local election officials across the country have raised questions about the day-to-day impact of the designation and how it will benefit their work to conduct accessible, accurate and secure elections. This document details DHS's critical infrastructure designation and what election administrators can expect moving forward. It also provides a glossary of terms frequently used in conjunction with correspondence and discussions about the critical infrastructure designation.

What is critical infrastructure?

Critical infrastructure is a DHS designation established by the Patriot Act and given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [i] DHS, the department responsible for critical infrastructure, was established by the Homeland Security Act in 2002.

In order to fulfill its responsibilities under the Patriot Act, DHS uses the National Infrastructure Protection Plan (NIPP) as the foundational document, or "rule book," for how to develop sector-specific critical infrastructure plans. The NIPP established a process roadmap by which the nation's critical infrastructure sectors can be identified and created.

In addition to the Patriot Act and NIPP, a third piece of critical infrastructure governing authority comes from Presidential Policy Directive 21 (PPD-21). Released on February 12, 2013, PPD-21 established the Federal Government's "strategic imperatives" in its approach to the nation's critical infrastructure. It established the current critical infrastructure sectors and identified each sector's Sector Specific Agency (SSA), which is the agency charged with structuring and managing the sector.

What other sectors are included in the nation's critical infrastructure?

Critical infrastructure sectors are groupings based on common function and form. There are currently 16 sectors. They are: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Waste; Transportation Systems; and Water and Wastewater Systems. [ii]

One critical infrastructure sector, Government Facilities, has three sub-sectors, Elections, National Monuments and Icons, and Education Facilities. Subsectors are sections of a specific sector that vary from the rest of the sector substantially enough to justify creating a plan just for the subsector.

How are sectors organized?

Once DHS creates a sector, the SSA structures it and helps it self-organize, a requirement of the NIPP. With regard to election systems, this means that members of the election community come together to join and manage the various components that make up this sector. After the critical infrastructure sector is formally established and organized, the SSA is charged with managing it. The SSA is "responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment." [iii]

While DHS has vast national security knowledge and resources, it acknowledges that it is not an issue-area expert for some of the sectors designated as critical infrastructure. To fill this knowledge gap, DHS will often appoint another federal agency as its Co- Sector Specific Agency (Co-SSA). This is especially common when DHS creates a subsector. Co-SSAs help DHS navigate the nuances of a specific subsector and share SSA responsibilities. For example, the sub-sector Co-SSA for Education Facilities is the Office of Safe and Drug-Free Schools in the Department of Education. A complete list of the sectors, and their respective SSAs and Co-SSAs follows at the end of this document (Addendum II).

DHS has yet to designate a Federal Agency as a Co-SSA for the elections sector. The U.S. Election Assistance Commission (EAC) has publicly called on DHS to select the commission to fill this important role. The request was made in light of the working relationship between DHS and the EAC, crafted during the 2016 presidential election and continued since.

Beyond the SSA and Co-SSA roles, there are other key entities established to support a newly designated critical infrastructure sector, including:

- ✓ **Sector Coordinating Councils (SCCs)**: These are "self-organized, self-run, and self-governed private sector councils consisting of owners and operators and their representatives, who interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience policy coordination and planning and a range of related sector-specific activities." [iv]
- ✓ **Government Coordinating Councils (GCCs)**: These consist of "representatives from across various levels of government (including Federal and State, local, tribal and territorial), as appropriate to the operating landscape of each individual sector, these councils enable interagency, intergovernmental,

and cross-jurisdictional coordination within and across sectors and partner with SCCs on public-private efforts." [v]

As part of its designation plan, the SSA will work to establish these councils to support the U.S. election systems designation. For the U.S. election system, these groups will likely include representatives from federal, state, and local government; election system vendors; and other stakeholders impacted by the critical infrastructure designation.

Another key component of operating a critical infrastructure sector is to ensure clear, strong lines of communication between the SSA, Co-SSA, coordinating councils, and stakeholders. This can include creation of the following:

- ✓ **Information Sharing and Analysis Centers (ISACs)**: These are "operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders." (Source: Presidential Decision Directive 63, 1998)[vi]
- ✓ **Information Sharing and Analysis Organizations (ISAOs):** Though similar to ISACs, ISAOs are "any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of: (a) Gathering and analyzing Critical Infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof; (b) Communicating or disclosing Critical Infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to Critical Infrastructure or protected systems; and (c) Voluntarily disseminating Critical Infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (a) and (b)." [vii]

The distinction between an ISAC and an ISAO is that "[u]nlike ISACs, ISAOs are not directly tied to Critical Infrastructure sectors, as outlined in Presidential Policy Directive 21. Instead, ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest such as small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc." [viii] Essentially, ISAOs allow for more widespread information sharing across sectors and among interested individuals regardless of clearance, knowledge level, or inclusion in a critical infrastructure sector.

What is unique about the protection of critical infrastructure communications?

Information about security and vulnerabilities that is shared under the restrictions of the Critical Infrastructure Information Act is considered Protected Critical Infrastructure Information (PCII). PCII is not subject to the many disclosure regulations, such as those found in the Freedom of Information Act and its state-level counterpart. This protection, allows the critical infrastructure community to discuss vulnerabilities and problems without publically exposing potentially sensitive information.[ix]

For those participating in election sector coordinating councils this protection means that some information communicated between DHS and the coordinating councils can be protected. This limits the potential for sensitive election security information to be made public and protects potentially sensitive material from being misconstrued or used for nefarious purposes. This protection is made possible by an exception to the Federal Advisory Committee Act created by the Critical Infrastructure Partnership Advisory Council.[x]

Are new resources available following a critical infrastructure designation?

A critical infrastructure designation provides for greater access to DHS information and security resources. It also provides a safer and more discreet exchange of information and requests for advice or assistance. While it is important to note that DHS will provide assistance to any domestic entity that requests help and not just critical infrastructure, its assistance to entities within a critical infrastructure sector is prioritized over providing assistance to non-critical infrastructure entities.

DHS resources – including on-going and current information about threats, risk and vulnerability assessments, and security best practices as well as hands-on advice – help infrastructure owners and managers better secure their systems. The department emphasizes the importance of the information assets it has available to critical infrastructure entities and understands that security clearances are a requirement for accessing some of these resources. This is why DHS works with infrastructure owners and managers to secure clearances when necessary.

Use of DHS resources and participation in sector councils is voluntary, and DHS continually states that it cannot force critical infrastructure owners and managers to interact with a sector, its components, or its resources. Entities that choose to leverage these new resources have a direct line to DHS resources via a Cyber Security and Protective Security Advisor. These advisors directly supply security assistance to the country and handle on-going assistance to CI entities.

While some within the election community remain skeptical about the critical infrastructure designation, their outstanding concerns about the designation make the case for why input from key election sector stakeholders is a vital part of setting up the needed infrastructure of councils and committees that can make this designation impactful. DHS is actively seeking participation from election stakeholders and their sector

allies, noting that there is an advantage inherent in helping to shape the critical infrastructure mechanisms election officials will use to gain resources and communicate with DHS. The department has relied on the EAC to provide the forum for much of this outreach, and the commission recommends that election officials and others in the election community take steps to becoming involved in this process either directly or through the EAC.

What role will the EAC play as DHS stands up the critical infrastructure designation?

The EAC has requested DHS name the commission as Co-SAA. This designation is important to ensure that state and local election officials and administrators have an informed federal advocate working directly with DHS as the department determines what resources and services are needed to protect U.S. election systems and how these resources will be distributed. The EAC has held and will continue to hold, hearings and meetings to give DHS a platform to discuss the designation and its potential benefits, as well as answer questions from stakeholders. The EAC prides itself on serving as a trusted intermediary between state and local election officials and federal government leaders, as well as a provider of resources needed to navigate this new space. Serving as the official Co-SSA for implementing the critical infrastructure designation would tap into this strength and provide election officials with assurance that their interests and concerns will shape the contours of DHS's plan moving forward.

Addendum I: Glossary of Key Terms and Acronyms

Critical Infrastructure Glossary

Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source:§1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e)))
Critical Infrastructure Partnership Advisory Council (CIPAC)	Council established by DHS under 6 U.S.C. §451 to facilitate effective interaction and coordination of critical infrastructure activities among the Federal Government, the private sector, and State, local, tribal and territorial governments. (Source: CIPAC Charter) These meetings are exempt from the Federal Advisory Committee Act (FACA) requirements that they be open to the public and provide meeting materials to the public.
Critical Infrastructure Sector	A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; NIPP 2013 addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)
Cybersecurity	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: 2009 NIPP)
Executive Order 13636	Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity framework; and promote and incentivize the adoption of strong cybersecurity practices. (Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013)
Government Coordinating Council (GCC)	The government counterpart to the Sector Coordinating Council for each sector established to enable interagency and intergovernmental coordination; comprises representatives across various levels of government (Federal and State, local, tribal and territorial) as appropriate to the risk and operational landscape of each sector. (Source: 2009 NIPP)
Information Sharing and Analysis Centers (ISACs)	Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (Source: Presidential Decision Directive 63, 1998) ISACs are not operated, controlled, or managed by DHS.

Information Sharing and Analysis Organization (ISAO)	"Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability there of; communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure or protected systems; and voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B)." (Source: Homeland Security Act of 2002)
Infrastructure	The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (Source: DHS Lexicon, 2010)
National Annual Report	Each SSA is required to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CI/KR protection in their respective sectors. (National Infrastructure Protection Plan: The National CI/KR Protection Annual Report)
National Infrastructure Coordinating Center (NICC)	The National Infrastructure Coordinating Center (NICC) is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between the Department of Homeland Security and the owners and operators of our nation's infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets. (Source: DHS.gov/national-infrastructure-coordinating-center)
National Infrastructure Protection Plan (NIPP)	The National Infrastructure Protection Plan 2013, involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry, provides a clear call to action to leverage partnerships, innovate for risk management, and focus on outcomes, provides an updated approach to critical infrastructure security and resilience, and involves a greater focus on integration of cyber and physical security efforts. (DHS, NIPP Fact Sheet)
National Protection and Programs Directorate (NPPD) – (DHS/NPPD)	[The DHS division] that leads the DHS mission to reduce risk to the Nation's critical physical and cyber infrastructure through partnerships that foster collaboration and interoperability. (Source: DHS FY13 Budget Guidance). NPPD contains the Federal Protective Service, the Office of Identity Management, the Office of Cybersecurity and Communications, the Office of Cyber and Infrastructure Analysis, and the Office of Infrastructure Protection.

Presidential Policy Directive 21 (PPD-21)	[Presidential Directive that] Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with owners and operators and State, local, tribal and territorial entities to enhance the security and resilience of critical infrastructure. (Source: PPD-21, 2013)
Presidential Policy Directive 8 (PPD-8)	[Presidential Directive that] facilitates an integrated, all-of-Nation approach to national preparedness for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters; directs the Federal Government to develop a national preparedness system to build and improve the capabilities necessary to maintain national preparedness across the five mission areas covered in the PPD: prevention, protection, mitigation, response, and recovery. (Source: PPD-8, 2011)
Protected Critical Infrastructure Information (PCII)	PCII is [information and communications] protected from disclosure. All critical infrastructure information that has been properly submitted and validated pursuant to the Critical Infrastructure Information Act and implementing directive; all information submitted to the PCII Program Office or designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise. Critical infrastructure information voluntarily shared with the government and validated as PCII by the Department of Homeland Security is protected from, the Freedom of Information Act (FOIA), State, local, tribal, and territorial disclosure laws, use in regulatory actions and use in civil litigation. PCII can only be accessed in accordance with strict safeguarding and handling requirements, and only trained and certified federal, state, and local government employees or contractors may access PCII.(Source: CII Act of 2002, 6 U.S.C. § 131, and www.dhs.gov/pcii-program)
Protective Security Advisors (PSAs)	Trained critical infrastructure protection and vulnerability mitigation subject matter experts who work for DHS and are responsible for ensuring all Office of Infrastructure Protection critical infrastructure security and resilience programs and services are delivered to State, local, tribal, and territorial stakeholders and private sector owners and operator. There are three types: (1) Regional Directors, supervisory PSAs, PSAs, and geospatial analysts. s. (Source: DHS.gov/protective-security-advisors)
Sector Coordinating Council (SCC)	The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. They serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (Source: Adapted from the 2009 NIPP)
Sector-Specific Agency (SSA)	A Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise, as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (Source: PPD-21, 2013)

Sector-Specific Plans (SSP)	Planning documents that complement and tailor application of the National Infrastructure Protection Plan to the specific characteristics and risk landscape of each critical infrastructure sector. SSPs are developed by the SSAs in close collaboration with the SCCs and other sector partners. (Source: Adapted from the 2009 NIPP)

Addendum II: Critical Infrastructure Sectors and their SSAs and Co-SSAs

Sector/ Subsector	SSA	Co-SSA
Chemical	Department of Homeland Security (DHS)	
Commercial Facilities	Department of Homeland Security (DHS)	
Communications	Department of Homeland Security (DHS)	
Critical Manufacturing	Department of Homeland Security (DHS)	
Dams	Department of Homeland Security (DHS)	
Defense Industrial Base	Department of Defense (DOD)	
Emergency Services	Department of Homeland Security (DHS)	
Energy	Department of Energy (DOE)	
Financial Services	Department of the Treasury	
Food and Agriculture	Department of Agriculture (USDA)	Department of Health and Human Services (HHS)
Government Facilities	Department of Homeland Security (DHS)	General Services Administration (GSA)
Elections (subsector)	Department of Homeland Security (DHS)	
Education Facilities (subsector)	Department of Homeland Security (DHS)	Department of Education
National Monuments (subsector)	Department of Homeland Security (DHS)	Department of the Interior (DOI)
Healthcare and Public Health	Department of Health and Human Services (HHS)	
Information Technology	Department of Homeland Security (DHS)	
Nuclear Reactors, Materials, and Waste	Department of Homeland Security (DHS)	
Transportation Systems	Department of Homeland Security (DHS)	Department of Transportation (DOT)
Water and Wastewater Systems	Environmental Protection Agency (EPA)	

[i] Patriot Act, (Sec. 1016(e))
[ii] https://www.dhs.gov/Critical-Infrastructure-sectors, accessed May 2, 2017.
[iii] Ibid.
[iv] Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, p. 12.
[v] *NIPP 2013*, p. 31.
[vi] Presidential Decision Directive 63, 1998.
[vii] Source: *Homeland Security Act of 2002, 6 U.S.C. § 131.*
viii Department of Homeland Security, Frequently Asked Questions About Information Sharing and Analysis Organizations (ISAOs), https://www.dhs.gov/isao-faq, accessed May 3, 2017.
[ix] Department of Homeland Security, *NIPP 2013*, p. 12.
[x] Department of Homeland Security, *United States Department of Homeland Security Charter of the Critical Infrastructure Partnership Advisory Council*, https://www.dhs.gov/sites/default/files/publications/cipac-charter-11-30-16-508.pdf, accessed June 5, 2017

Harvard Kennedy School Belfer Center
Campaign Cybersecurity Playbook

November 2017

HARVARD Kennedy School
BELFER CENTER

REPORT - *Belfer Center for Science and International Affairs, Harvard Kennedy School*

Cybersecurity Campaign Playbook

November 2017

Welcome

People join campaigns for different reasons: electing a leader they believe in, advancing an agenda, cleaning up government, or experiencing the rush and adrenaline of campaign life. These are some of the reasons we got involved in politics. We certainly didn't sign up because we wanted to become cyber experts and we're guessing you didn't either.

We come from different political parties and don't agree on much when it comes to public policy, but one thing uniting us is the belief that American voters should decide our elections and no one else. Our increasingly digital way of living and working offers new ways for adversaries to influence our campaigns and elections. While you don't need to be a cyber expert to run a successful campaign, you do have a responsibility to protect your candidate and organization from adversaries in the digital space. That's why Defending Digital Democracy, a project of Harvard Kennedy School's Belfer Center for Science and International Affairs, created this **Cybersecurity Campaign Playbook [PDF]**.

The information assembled here is for any campaign in any party. It was designed to give you simple, actionable information that will make your campaign's information more secure from adversaries trying to attack your or-ganization—and our democracy. Most of all,

Table of Contents

I. Welcome
Top 5 Checklist
The Playbook Approach

II. Introduction
The Vulnerable Campaign Environment
The Threats Campaigns Face

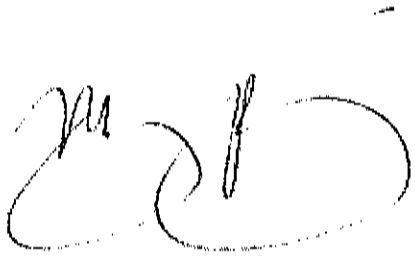
III. Managing Cyber Risk

IV. Securing Your Campaign

V. Steps to Securing Your Campaign
Handouts for Staff & Family Members
Step 1: The Human Element
Step 2: Communication
Step 3: Account Access and Management
Step 4: Incident Response Planning
Step 5: Devices
Step 6: Networks

we hope this resource allows you to spend more time on what you signed up for—campaigning.

Good luck.



Robby Mook
Hillary Clinton 2016 Campaign Manager

Matt Rhoades
Mitt Romney 2012 Campaign Manager

P.S. Do you see a way to make the Playbook better? Are there new technologies or vulnerabilities we should address? We want your feedback. Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #CyberPlaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

VI. Authors & Contributors

Top Five Checklist

1. Set the Tone:

Take cybersecurity seriously. Take responsibility for reducing risk, train your staff, and set the example. Human error is the number one cause of breaches.

2. Use the cloud:

A big, commercial cloud service will be much more secure than anything you can set up. Use a cloud-based office suite like GSuite or Microsoft365 that will provide

all your basic office functions and a safe place to store information.

3. Use two-factor authentication:

Require 2FA for all important accounts, including your office suite, any other email or storage services, and your social media accounts. Use a mobile app or physical key for your second factor, not text messaging.

4. Create strong, long passwords:

For your passwords, create SOMETHINGREALLYLONGLIKETHISSTRING, not something really short like Th1$. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with L0t$ 0f $ymB01$. A password manager can help, too.

5. Plan and prepare:

Have a plan in case your security is compromised. Know whom to call for technical help, understand your legal obligations, and be ready to communicate internally and externally as rapidly as possible.

The Playbook Approach

This Cybersecurity Campaign Playbook was written by a bipartisan team of experts in cybersecurity, politics, and law to provide simple, actionable ways of countering the growing cyber threat.

Cyber adversaries don't discriminate. Campaigns at all levels – not just presidential campaigns – have been hacked. You should assume you are a target. While the recommendations in this playbook apply universally, it is primarily intended for campaigns that don't have the resources to hire professional cybersecurity staff. We offer basic building blocks to a cybersecurity risk mitigation strategy that people without technical training can implement (although we include some things which will require the help of an IT professional).

These are baseline recommendations, not a comprehensive reference to achieve the highest level of security possible. We encourage all campaigns to enlist professional input from credentialed IT and cybersecurity professionals whenever possible.

Introduction

Candidates and campaigns face a daunting array of challenges. There are events to organize, volunteers to recruit, funds to raise, and the relentless demands of the modern media cycle. Every staffer must anticipate unfortunate surprises like gaffes or a last-minute attack ad. Cyber attacks now belong on this list as well.

As campaigns have become increasingly digital, adversaries have found new opportunities to meddle, disrupt, and steal. In 2008, Chinese hackers infiltrated the Obama and McCain campaigns, and stole large quantities of information from both. In 2012, the Obama and Romney campaigns each faced hacking attempts against their networks and websites. In 2016, cyber operatives believed to be sponsored by Russia stole and leaked tens of thousands of emails and documents from Democratic campaign staff.

The consequences of a cyber breach can be substantial. News of a breach itself, compounded by a slow-drip release of stolen information, can derail a candidate's message for months. Attackers overloading a website can lead to lost donations at key moments. The theft of personal donor data can generate significant legal liabilities and make donors reluctant to contribute to a campaign. Destructive attacks aimed at staff computers or critical campaign servers can slow down campaign operations for days or even weeks. Cleaning up the resulting mess will divert precious resources in the heat of a close race, whether it's for president or city council.

For the foreseeable future, cyber threats will remain a real part of our campaign process. As democracy's front line, campaign staff must recognize the risk of an attack, develop a strategy to reduce that risk as much as possible, and implement response strategies for that moment when the worst happens. While no campaign can achieve perfect security, taking a few simple steps can make it much harder for malicious actors to do harm. Ironically, the most sophisticated state actors often choose the least sophisticated methods of attack, preying on people and organizations who neglect basic security protocols. That is our primary reason for creating this Cybersecurity Campaign Playbook.

In today's campaigns, cybersecurity is everyone's responsibility. Human error has consistently been the root cause of publicized cyber attacks, and it's up to the candidate and campaign leaders to weave security awareness into the culture of the organization. The decisions humans make are just as important as the software they use. Going forward, the best campaigns will have clear standards for hard work, staying on message, being loyal to the team—and following good security protocol.

Before we get into our recommendations, let's quickly frame the problem:

- the **environment** in which your campaign is operating;
- the **threats** your campaign will likely face; and,
- the **importance** of cyber risk management.

The Threats Campaigns Face

Unfortunately for campaigns and our country, foreign adversaries may think that harming or helping a particular candidate advances their national interest, whether that means creating chaos and confusion among American voters, or punishing an official who has spoken out against them. This may sound like thriller fiction, but the reality is that a sophisticated foreign intelligence service, cybercriminal or hacktivist with a grudge against a candidate, could decide that you or someone on your campaign is a target.

These are the sorts of threats managers and staffers have to realize are possible.

WHO'S HACKING?

Campaigns face information and cybersecurity threats from a wide array of actors. Lone "black hat" hackers and cybercriminals have

tried compromising campaigns for reasons of personal gain, notoriety, or the simple desire to see if they could. Nation-states pose the most dedicated and persistent threat. Russian espionage groups known as "Fancy Bear" (APT 28) and "Cozy Bear" (APT 29) were implicated in the 2016 campaign hacks. The Chinese have focused much more on information gathering. They are believed to have been active in the 2008 and 2012 presidential campaigns, but there is no evidence they released any stolen materials. The North Koreans infamously retaliated against Sony Pictures Entertainment for producing the film, The Interview, by stealing and releasing company emails and wiping their systems. Heightening tensions with the United States could prompt more attacks in the future.

Managing Cyber Risk

Risk is best understood in two parts. First, there are **vulnerabilities**: weaknesses in your campaign that make information susceptible to theft, alteration, or destruction. Vulnerabilities can originate in hardware, software, processes, and in the vigilance of your staff. Second are the actual **threats**: the nation states, hacktivists, and other nonstate groups with the capability to exploit those vulnerabilities. Risk results where threat and vulnerability meet.

There's nothing you or your campaign can do to prevent threats themselves – they are the result of larger geopolitical, economic, and social forces. What you can do is substantially reduce the likelihood that your adversaries will succeed by reducing how vulnerable you are. Reducing vulnerability reduces risk – it's up to you to decide which ones are most essential to reduce. For example, you may decide that the most damaging thing a hacker could do is to steal your candidate's self research report, so you will devote extra resources for secure cloud-based storage, require long passwords and restrict access to a small number of people. You may decide to make other documents on the campaign more widely available and less secure, since more people need them to do their job and they wouldn't cause much damage if they were leaked.

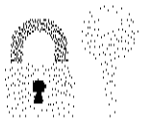
There are technical aspects to risk mitigation and we have many technical recommendations in this playbook, but what matters most is your holistic approach. As a campaign leader, the most important thing you can do is make fundamental choices, such as who has access to information, what information is kept or discarded, how much time you devote to training, and your own behavior as a role model. As a campaign professional, risk management is your responsibility –

both technical and human. It's up to you to decided what data and systems are most valuable and what resources you commit to protect it.

Securing Your Campaign

Our security recommendations are organized according to three principles:

1. Prepare: The success of nearly every one of the Playbook's recommendations depends on the campaign manager creating a culture of security vigilance that minimizes weak links. That means establishing clear ground rules that are enforced from the top down and are embraced from the bottom up.



2. Protect: Protection is critical. When you discover you have a security problem, it is already too late. Building the strongest defenses that time and money allow is key to reducing risk. Internet and data security works best in layers: there is no single, bulletproof technology or product. A few basic measures used in combination can make a campaign's digital architecture more difficult to breach and more resilient if compromised.

3. Persist: Campaigns now face adversaries with ever-increasing levels of resources and expertise; even the most vigilant culture and the toughest infrastructure may not prevent a security breach. Campaigns need to develop a plan ahead of time to deal with a breach if one occurs.

Some campaigns have more time and money for cybersecurity than others. That's why our recommendations offer two tiers of protection: "**good**" and "**enhanced.**" The "good" tier represents everything a campaign **must** do to have a **minimum** level of security. Using the "good" recommendations in a piecemeal fashion will leave you vulnerable. You should always aspire to do more as time, money, and people allow, which is why we recommend using the "enhanced" level whenever possible. If you have the resources to get reputable, trained IT support, it's money well spent. Threats are constantly evolving and professional IT services will help get you beyond what this playbook provides and keep you abreast of the latest threats and solutions.

Management

Campaign managers need to take responsibility for their cybersecurity strategy, but most will delegate development and supervision to a deputy or operations director. It's important that cybersecurity is tightly integrated into HR and IT work, since correctly onboarding staff, provisioning hardware, and controlling permissions will be critical to your strategy. Many small campaigns will rely on volunteer support for IT and cybersecurity. You can use this playbook to guide your discussion with your volunteer support. The key is to carefully vet the volunteers who

support you and carefully control access, so that volunteer support doesn't create new vulnerabilities. You should make sure a campaign staffer is supervising IT work and controlling permission to access different systems.

When To Start

Whatever support model you have, *cybersecurity should start on Day One*. What follows is a "top five checklist" of measures that are absolutely vital. Make sure these are in place at the very beginning, even if there are just one or two staff, then complete the other "good" recommendations as soon as possible.

Cost

A lot of what we recommend here is free or very low cost. In fact, everything on our top five list is free, except getting a cloud-based platform, which will only cost a few dollars per month per employee. High target campaigns will need to budget enough resources for hardware and software to execute a responsible strategy, but this should still be a very small percentage of a multi-million dollar statewide campaign budget. Smaller campaigns will be able to execute the recommendations here for a few hundred to a few thousand dollars depending on how many staff or volunteers work on the campaign.

Any references to vendors and products are intended to help provide examples of common solutions, but do not constitute endorsements. If challenges arise when implementing products or services, we encourage you to reach out directly to the vendors, who can usually provide user-level technical assistance. When it comes to product and service selection, we encourage every campaign to consult with a cybersecurity expert or conduct independent research to find the best product for their needs.

The Vulnerable Campaign Environment

Today's campaigns are uniquely soft targets. They're inherently temporary and transient. They don't have the time or money to develop long-term, well-tested security strategies. Large numbers of new staff can be on-boarded quickly without much time for training. They may bring their own hardware from home – and the malware lurking on it! Things move fast, the stakes are often high, and people feel like they don't have the time to care about cybersecurity. There are a lot of opportunities for something to go wrong.

At the same time, campaigns rely more and more on proprietary information about voters, donors, and public opinion. They also store sensitive documents like opposition research, vulnerability

studies, personnel vetting documents, first-draft policy papers, and emails. The risks of a potential attack are increasing and so are the consequences.

THE DANGER OF AN ATTACK

Picture this: It's a month before Election Day, and the race is tight. You arrive at headquarters early, fire up the coffee maker, get to your desk, and log into your computer. A black screen pops up, then a gruesome cartoon of your candidate, followed by a message. Your hard drives have been wiped clean. Every digital bit of information you've gathered—memos, targeting lists, balance sheets—is gone. Getting it back, you read, will cost a cool million in Bitcoin and the renunciation of a major policy position.

An unidentified group hacked into your computer months ago, and has been quietly stealing emails, strategy memos, donors' addresses, and staffers' Social Security numbers. The group has spent weeks combing through the bounty in search of dirty laundry and created an easy-to-use website dedicated solely to distributing the highlights. Prominently featured is a lengthy "self research" book on your candidate. For now, the campaign's website is down, its social media accounts have been suspended for pushing out lewd images, and there's not a working computer in sight.

Steps to Securing Your Campaign

STEP 1: The Human Element

Cybersecurity is fundamentally a human problem, not a technical one. The best technical solutions in the world will have no effect if they are not implemented properly, or if they are not continuously updated as technology evolves. Successful cybersecurity practices depend upon creating a culture of security.

1. Establish a strong information security culture that emphasizes security as a standard for a winning campaign. Just as campaign staffers are instructed not to take an illegal donation, employees should know to avoid clicking on links or opening attachments in emails from unknown senders.
   - Onboarding: Provide basic **information security training** when you onboard new staff. You can distribute the Staff Handout at your training.
   - Trainings: Make security part of all your ongoing **staff trainings**, such as senior staff retreats or GOTV trainings. Provide **additional training** for those in sensitive roles, such as the candidate, press staff, senior staff, and anyone with system administrator privileges on your network. Managers should require that the most important people in the campaign—including the candidate—have their security settings checked by whoever runs IT (that may be the manager herself). Don't be timid or half-hearted about security for the candidate and other VIPs!
   - Set the example: Senior campaign staff and the candidate must take a **visible leadership role**, advocating for cybersecurity during trainings. Senior staff should provide **periodic reinforcement** of cybersecurity's importance to junior staff in meetings and on calls. Don't just have technical experts conduct trainings. The campaign manager or operations director can be a more powerful messenger precisely because they're seen as less "technical."
2. Conduct a thorough **vetting** of staff, volunteers, and interns—anyone requesting access to campaign information—to avoid giving credentials to someone who wants to steal or sabotage your systems. Establish a definition for **sensitive information** and rules for its use. For example, you could choose to classify all polls, research materials, strategy memos, and related emails as "sensitive." Prohibit the transfer of sensitive information on communication channels that aren't managed and secured by the campaign. You can require that it be transferred only through encrypted messaging (see Step 2).
3. **Confirm that consultants and vendors with access to sensitive information have secure email and storage** (see Step 2). When in doubt, require vendors and consultants to use an account on your cloud-based office suite (See Step 2).
4. **Control access** to important online services, such as the official campaign social media accounts, to prevent use by unauthorized individuals. Make sure that those who leave the campaign can no longer access campaign-related accounts. You can do this easily by using a social media account management tool that acts as a gateway to all your accounts. If someone leaves the campaign, you should immediately disable their account.
5. **Educate staffers about the phishing threat**. Make sure they know how to spot and avoid suspicious links and emphasize the importance of identifying and reporting potential phishing

attacks. As part of the campaign's strong security culture, senior staff should recognize and praise anyone who reports suspicious behavior on their system or admits to clicking a potentially malicious link.

Handouts

For Staff Members

For Family Members

1. Software products such as Phishme and KnowBe4 can **train your staff by sending them fake phishing emails**. This is a safe, quick, and effective way to learn who is at risk of clicking a link, so you can give them counseling and extra training. Many of these products also filter some phishing attempts out of your email.
2. If you have the resources, **hire a dedicated IT professional** to manage your campaign's systems and an IT security expert to help protect, maintain, and monitor your campaign's digital infrastructure. He or she can provide regular security training and testing of your people and systems, while customizing security solutions.
3. **Contract with a cybersecurity firm** to provide security solutions, review your defenses, and/or monitor your systems for a breach. Know which firm you want to contact if you are breached and need urgent incident response support. This is an alternative to hiring a full-time IT security expert. Do your research and go with a highly reputable, U.S.-based firm—not all cybersecurity firms provide the same level of service.

WORKING WITH SECURITY PROFESSIONALS

If you decide to work with a security professional, how will you evaluate the right person or firm? Whether it's through personal recommendations or positive public reviews, it's important that you avoid costly yet ineffective support. When interviewing potential security professionals, ask about how they've responded to past security incidents and how they've enabled others to work more securely. Your respective national party committee or trusted campaign professionals may be able to recommend options to

choose from. Bear in mind that culture affects security and that even the best recommendations may fail to achieve results if they are not followed (i.e., just hiring a firm won't solve your problems).

STEP 2: Communication

Not all methods of communication are equally secure, so use the most secure method possible. Campaign leadership should set a standard that encourages in-person conversations whenever possible, and discourages needless or superfluous emails. Whether it is phone calls, texting, or emailing, different products and services offer different levels of protection, so do your research before you choose which systems your campaign is going to use.

WHAT IS THE CLOUD?

"Cloud services" provide management and access to information stored remotely on the Internet. They run on off-site servers managed by third-party companies; this includes many common services you may already use, such as Gmail or Dropbox. It's good to store information in the cloud instead of on your personal computer because big cloud providers have the money and expertise to make their server farms more secure than your laptop's hard drive, or an office server. **It's like the difference between leaving cash under your mattress and storing it in a bank's security vault.** Using cloud services offers an additional backstop against data loss if an individual device is lost or compromised. Cloud storage is a feature included in comprehensive office security services such as GSuite and Microsoft365. Other services include Dropbox or Box.

1. Use a **cloud-based office suite** that provides secure email communication, document creation, chat, and file sharing, such as GSuite or Microsoft365. For example, GSuite includes Google Drive for file sharing, Gmail for email hosting, Google Hangouts for chat, and Google Docs for word processing, spreadsheets, and presentations. Microsoft365 offers OneDrive/SharePoint for file sharing, Outlook/Exchange for email, Microsoft Teams for chat, and Microsoft Office for word processing, spreadsheets, and presentations. Cloud-based systems managed by major firms will be better protected than any servers you could set up in your campaign. There are free versions of both products, but the paid versions give you many more administrative capabilities. Google also offers a service called *Protect Your Election* that will provide extra protection against phishing for their free email service.They also offer a free service to protect your website against disabling attacks.

2. Use the most secure systems possible for communication.
   - Use **encrypted messaging** services such as Signal, Wickr, especially for messages, document sharing and phone calls. Many campaigns require that sensitive information only be transmitted by encrypted messaging, although you can use it for all communication if you want (this is especially smart for high-risk individuals like the candidate). Signal and Wickr allow you to auto-delete messages, which reduces risk.
   - Switch off archiving for messaging services, such as Google Chat and Slack, so that old chats can't be stolen later. This requires going into "settings" and adjusting "retention policy" timelines. Some services require you to do this for every single chat conversation. We recommend retaining chat messages for one week or less.

3. Defend your email
   - **Turn on Auto-delete** in your email application for old emails to reduce the number of emails that could potentially be stolen. This usually requires going in and changing "retention policy" to shorter time periods in "settings." To ensure emails do not just sit in a "deleted items" folder, adjust settings to auto purge "deleted items" folder after a certain time period. We recommend retaining emails for one month or less.

4. Secure personal accounts
   - Campaign business should never go on personal accounts. However, adversaries will target personal accounts for hacking, so have your staff use strong passwords and two-factor for their personal accounts as well (this is included in our Staff Handout).

WHAT IS ENCRYPTION?

Encryption is a way of encoding information when it travels between users, or when it's stored, so it can't be read by anyone but the intended recipient. Think of it this way: a user "scrambles" the

data when she sends it and only the intended recipient has the key to unscramble it. Using encryption is smart, especially for sensitive information, because even if an adversary steals the data, it's unlikely they'll be able to read it. Most apps that use encryption, like Signal or Wickr, make the process seamless. Laptops or cloud storage systems use encryption as well.

STEP 3: Account Access and Management

One of the most challenging aspects of security is keeping unauthorized people out. This means preventing adversaries from gaining access to your data and preventing people within your campaign from having access to information they do not need. While some of the recommendations below may seem cumbersome, hackers depend on those who value convenience over security.

WHAT IS TWO-FACTOR AUTHENTICATION?

Two-factor authentication is a second layer of security that requires a user to provide an extra credential beyond her or his password. The second factor is critical because, if your password is stolen, an adversary still can't log into your account. Your password is something you know and your second factor is something you have, like a code that's generated by an app, a physical key, or even something biometric, like a fingerprint.

1. Require **two-factor authentication** (2FA) on all systems and applications. **Avoid texting (SMS)** for two-factor authentication, because attackers can easily clone a phone number and get access to texts. There are several 2FA apps that work just as well as texting, such as Google Authenticator, Microsoft Authenticator, and Duo Mobile. You can also use a physical FIDO

("fast identity online") key that is inserted into your USB drive such as Yubikey or Feitian. The website "TwoFactorAuth.org" is a helpful guide to services that do and do not offer 2FA.

2. Passwords.
   - **Require strong passwords.** As we noted earlier, "make passwords that are long and strong." Current computing capabilities can crack a seven-character password in milliseconds. A 20-, or even 30-character password will take much longer for a hacker to crack. Choose a string of words that you can easily remember.
   - Use a different password for different accounts so a hacker can't break into multiple accounts if a single password is stolen.
   - If someone reaches out requesting a password or password reset, require the request to be made in person or over a video chat to ensure it is the actual campaign staff member or volunteer. Only share passwords in person or over short-lived encrypted messages. Never share passwords over email or store/distribute using a helpdesk system.
3. **Use password managers** such as LastPass, 1Password, or Dashlane to help you manage a lot of long, strong passwords easily. But ensure that your management system has a long, strong password and two-factor authentication. We don't currently recommend password managers built into browsers, which are often less secure than these standalone managers.
4. Create **separate accounts for administrators and users**, and severely restrict access to administrator accounts. Administrators should also have two separate campaign accounts—one used only for their admin duties and one that is their standard user account for all other campaign business. This will reduce the likelihood that an adversary will be able to compromise an administrator account, which would provide access to the entire network.
5. Conduct **periodic reviews** of who has access to different devices and networks. Immediately block access of people who leave the campaign. Immediately change passwords if suspicious activity is observed.

PASSWORD MANAGERS

Password managers are a way to store, retrieve, and generate passwords. Some even have the ability to auto-populate the password line on login pages. The password manager requires a password of its own to login, which becomes the one password you do have to remember. The risk, of course, is that if someone breaks into your password manager (it has happened), that person will have all of your passwords. But this risk is almost always far outweighed by the benefit of strong, unique passwords across all of

your accounts. For campaigns, password managers sometimes make sense for accounts that have multiple users, because the administrator can safely share access to them.

1. Create **user profiles** for different types of campaign staff that automatically grant the necessary level of access. Different types of employees—interns, field staff, campaign leadership—require access to different resources. Having predetermined profiles makes it easier to ensure that people are getting access only to what they need.

WHAT ARE ADMINISTRATORS?

In "IT speak," an "administrator" or "admin" has the ability to give people access or control to systems or information. For example, as the "admin" for an email system, you can create accounts, change passwords, and set requirements like password length and two-factor authentication for all accounts. In an office suite like GSuite or Microsoft 365, you can also create groups, such as the "Field Team" or "Comms Team." An admin's job is really important. If they do things right, information will be available only to people who need it, which is essential for security. This means that deciding who gets admin privileges is also a critical decision. Only a few, highly trusted people should be able to grant others access to information. If a staffer with "admin" privileges leaves the campaign, make sure to take away their privileges immediately!

STEP 4: Incident Response Planning

It's just as important to plan for responding to an attack as it is to develop a security strategy to prevent one. How you respond often has more to do with the ultimate outcome of an incident than

what was compromised. You should budget some time at strategic retreats or longer senior staff meetings to discuss what will happen if something does go wrong. Here's a checklist of the steps you should take

LEGAL

✔ **Identify outside counsel** you will retain in the event of a cyber incident, and discuss the response process with them at the outset of the campaign. In most cases, this will be the same person who represents your campaign on other matters, but ideally you would have someone who specializes in incident response on call, either pro bono or for a $0 retainer.

✔ Ask your lawyer to explain **your legal obligations** if data is stolen and what compliance measures you will need to have in place.

✔ Understand **your vendors' legal obligations** to notify you or others if they are hacked. Wherever possible, include strict notification requirements in your vendor contracts, since third parties are a frequent source of breaches.

✔ If you believe you've been breached, a best practice is for **your lawyer to oversee your response** under attorney-client privilege.

✔ Talk to your lawyer about the best way to **work with law enforcement if a breach occurs**. Every campaign will approach this differently.

TECHNICAL:

✔ Determine ahead of time **whom you will call for technical assistance** if you think you've been hacked. Your state caucus or national party committee can usually provide referrals.

✔ Choose **someone on the campaign who will interface with technical experts** in the event of a breach. This is ideally the same person who is already coordinating IT for the campaign. Managing an incident response can be overwhelming, so you want someone focused on the technical aspects who knows what they are doing. That way you can focus on communicating with stakeholders and the press.

OPERATIONS:

✔ Decide in advance who will be on your **Incident Response Team** (IRT) and who will participate in incident response meetings. It's important to include someone from your IT, legal, operations, and communications teams. If you're a small campaign and don't have full-time communications, IT, or operations support, plan to include any key staff who oversee campaign operations.

✔ Determine the **chain of command for decision-making** in the event of a breach, especially regarding communications. In many cases, this will be the campaign manager, but some managers may choose to delegate responsibility to someone else.

✔ Identify what **app or technology you will use to communicate** if you think your email has been breached (Signal and Wickr are two common options). Communication during a breach is essential, but you don't want your adversaries to know what you're saying—or even that you are responding to their actions.

COMMUNICATIONS:

✔ **Conduct scenario planning**. For many campaigns, this can be part of an existing strategy retreat. For bigger campaigns at higher risk, it may be necessary to have a dedicated meeting. Your scenario planning should include:

✔ **Identifying key internal and external stakeholders**, like your staff, volunteers, donors, and supporters. Know whom you need to contact if an incident occurs and rank them in order of priority. Develop a contact list and designate who will reach out to them.

✔ **Brainstorm the most damaging scenarios** and consider how your stakeholders and messaging may change for each one. Different scenarios could include:

- Rumors that your campaign has been hacked;
- Credit card and contact information for your donors is stolen;
- Ransomware and an extortion attempt are lodged against your campaign;
- Your systems are wiped and shut down;
- Someone's emails are stolen;

- Your adversary steals your administrator's credentials and every file on your campaign drive.

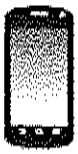
✔ **Be careful what you say in the present about cybersecurity policy** or cyber incidents. Some victims of cyber crimes have previously made grandiose pronouncements about their own security measures, or have criticized others who have been attacked. The press will hold you accountable for what you said in the past if you fall victim.

✔ Similarly, **avoid providing details about the scope of the event in the early phases** of the incident (and if you can avoid discussing the scope altogether, even better). Details available at the outset will change as you investigate. A common mistake is to say something that later turns out not to be true (e.g., "they didn't steal very much," or "no personal information was taken"). Saying only what you know for sure is the safest course. Statements should focus on the actions you are taking to make the situation right for the affected stakeholders.

✔ **Develop some boilerplate language** in advance, so that you can draft statements or talking points quickly if an incident occurs. At a minimum, create a simple Q & A document that you can rapidly revise if you actually need to use it. Creating a Q & A document in advance will help you to think as much about what you won't say as what you will say. For example, the first question will often be, "What happened?" However, you may not be able to answer that for days or weeks. The fact that you don't know what kind of breach will take place can actually help you write better boilerplate answers in advance. Questions to include in your Q & A document are [call out box]:

- What happened?
- How did it happen?
- Who did it?
- What was stolen or damaged?
- Was anyone's personal information stolen? What are you doing to protect them?
- How did the hackers do it?
- Are the hackers out of your system?
- How long were they in your system?
- What security measures did you have in place? Why weren't they effective?
- Shouldn't you have known this would happen? Why weren't your systems better secured?
- Are you working with law enforcement? Has law enforcement contacted you?
- In a ransomware breach, you'll be asked: Did you pay the ransom and why or why not?

✔ **Stay in touch with your key stakeholders** and keep them as informed as you can. You probably won't be able to say much, but contacting them regularly with what you do know, having a clear statement about your intentions, and providing details about what you are doing to manage the situation are key. Avoid setting an expectation of too frequent updates, because often you won't have new information and your stakeholders will become frustrated if you continue to return to them without new information. Only speak proactively to the media if you have new information to provide.



STEP 5: Devices

Every physical device in your campaign—from a cell phone, tablet, or laptop to a router, printer, or camera—represents a potential attack path into your network. A good cybersecurity plan will attempt to control access to, into, and on all devices. You can control access to devices by making sure they are always properly handled and accounted for. You control access into devices via two-factor authentication and strong passwords. You control the content on devices via encryption and the policies guiding how you store data (i.e., storing information in the cloud instead of on machines).

1. Always use the most **updated operating system** (OS) available, since system updates regularly include patches for the latest vulnerabilities. If possible, set device settings to **auto-install** these updates. Make it someone's job to check on a regular basis that everyone is current.
2. Use an automatic **cloud-based backup service** to mitigate the impact of data loss if a device is lost or stolen. Examples include Backblaze and CrashPlan.
3. Access to the device
   - From the start, campaign leadership should **create an environment** in which people take physical security of their devices seriously—losing a device could give an adversary access to critical information that can be used to hurt the campaign.
   - Although many campaigns cannot afford to buy new devices, it's always best to **purchase new equipment (especially computers and phones)** if you can. At a minimum, you should provide new devices for personnel who work with sensitive data.

- If staff are using their own computers and phones, **establish a "Bring Your Own Device" (BYOD) policy** that implements strong security practices (see endpoint protection below).
- Campaign members should **NOT use personal email accounts or devices that have not been secured per the BYOD policy** for campaign business, including email and social media. Any important information that resides outside devices or systems controlled by the campaign is vulnerable to attack. Leadership should constantly reinforce that campaign data needs to stay off personal email and unsecured computers.
- Report lost devices immediately. Require default settings that allow for **remote wiping** on all devices.
- Win or lose, have a plan in place for **what happens to all data, accounts, and devices** when the campaign ends. The immediate aftermath of a campaign is an especially vulnerable period.

4. Access into devices.
   - **Change default passwords and settings** on all devices. Many devices come from the factory with a default password that is really easy to guess. Also, disable the guest account if a device comes with one.
   - Implement **auto-lock** for phones and computers after two minutes and require a **password or fingerprint ID** to unlock.
   - Defender. There are special endpoint security apps for phones and tablets. Lookout is an example.

5. Content on devices.
   - Require **encryption** on all devices (computers and phones) to ensure that the loss of a device does not mean the compromise of its content. Examples include FileVault for Mac and BitLocker for Windows. Some devices like the iPhone do this by default, but not all do.
   - Install **endpoint protection** software on all devices. Some examples include Trend Micro, Sophos, and Windows Defender. There are special endpoint security apps for phones and tablets. Lookout is an example.

WHAT IS ENDPOINT PROTECTION?

Endpoints are the devices that staff use, including mobile phones, laptop computers, and desktop computers. They are the "endpoints" of the campaign's network, and staff are the "end users." Endpoint protection centrally controls and manages

security on remote devices. It's especially important for campaigns that allow staff to "bring your own device" (BYOD), since the campaign needs to ensure that the device is secure, free of malware, and can be wiped if stolen or lost. Endpoint protection can also monitor the device to make sure software is up to date and detect new malware or potential threats. For many campaigns, this will feel like a big lift, but building it into your routine onboarding and investing some time upfront can save you a lot of grief later.

1. Use **mobile device management (MDM) software**, which monitors activity to ensure all devices comply with the mobile phone and user device security policies you have established for your campaign. Examples include VMware AirWatch, Microsoft InTune, and JAMF. GSuite and Microsoft Office 365 also include an MDM service.
2. Use advanced threat protection services that monitor and alert for malicious activity, such as CrowdStrike Falcon or Mandiant FireEye. Crowdstrike sometimes offers Falcon breach prevention service pro bono through the Crowdstrike Foundation, depending on the needs of your campaign and campaign finance rules.

STEP 6: Networks

Networks are the system of physical hardware, digital software, and their connections. They represent another target-rich environment for attack. Network security comprises everything from how devices communicate with one another to using cloud services for data storage.

1. **Embrace the cloud. Store data on cloud services, not on personal computers or servers.** Anything stored on a personal device faces higher risk than the cloud.
   - No one should have access to all files on the network; accounts with comprehensive administrator access should not be used for day-to-day work. Divide your file storage into department folders and grant access accordingly.

- Ensure **access to shared content is by invitation only**. Some file management services also allow for implementing expiration dates on invitations and access.
- Periodically audit what is being shared and with whom.

2. Have a **separate "guest" wifi** network for visitors and volunteers that limits their access to campaign resources. Try to purchase routers that offer a "guest profile" that will automatically segment your network.
3. When traveling, or before you set up your campaign office, avoid public wifi services as much as possible and use trusted wifi networks wherever possible. If you need mobile wifi, then try to provide campaign staffers with mobile wifi hotspots for tethering. Public wifi is often free and easy to connect with, but attackers can also use it to penetrate your hardware.
   - Where possible, staffers should **use a VPN** (virtual private network). VPNs help protect against intruders when on public wifi. Examples of VPN services include ExpressVPN or TunnelBear. Not all VPNs are created equal. Beware of free services: many are looking to take your data!
4. **Secure your browser**. PC Magazine ranked Chrome and Firefox as the two safest browsers in 2017. Regardless of what browser you use, keep it up to date.

WHAT ARE VPNs?

A virtual private network (VPN) is an encrypted "tunnel" for your Internet traffic, hiding it from intruders. Some offices use it as a way to log remotely into the office network, but this isn't very common for campaigns. Campaigns should consider having their staff use a VPN on computers and mobile phones if they often have to use public wifi or untrustworthy networks (which is sometimes the case for traveling staff or field offices).

1. You can take more advanced steps to protect your network, but they should be implemented by an IT professional. We would suggest you ask them to include the following:
   - **Set up a hardware firewall**.
   - **Encrypt your wifi connection** using the WPA2 or 802.1x security protocols (do not use WEP).

- Configure cloud-based web proxies to **block access to suspicious sites** from any campaign-owned device, no matter where it is. Service provider examples include Zscaler, Cisco Umbrella and McAfee Web Gateway Cloud Service.
- Have your activity logs stored on a cloud service provider such as LogEntries or SumoLogic.
- **Segment your cloud-based storage** so that not everything is stored in the same place. Opposition research, strategy memos, and personnel files should be kept in different folders, and access to those folders should be restricted to the people who really need them. Consider a different storage system entirely for your campaign's most sensitive information. Restrict access so that only key personnel can access it, and only when using specific devices. (For example, if you use Microsoft365 for your office suite and document storage, but your most sensitive documents on a Dropbox or Box account.) If a member of the campaign becomes compromised, this kind of segmentation can limit the damage.

2. **Train staff not to connect their devices to unknown ports or devices.** Don't use public chargers at airports or events. Don't accept free phone chargers or batteries at events (that free USB drive may be loaded with malware!).

Authors & Contributors

This project was made possible by dozens of people who generously volunteered their time. Special thanks are due to Debora Plunkett for leading the project and Harrison Monsky for writing the document. We are also indebted to the people listed below who invested countless hours in reviewing drafts and providing input.

Defending Digital Democracy
Eric Rosenbach, Co-Director, Harvard Kennedy School Belfer Center
Robby Mook, Belfer Center Fellow
Matt Rhoades, Belfer Center Fellow
Heather Adkins, Director, Information Security and Privacy, Google
Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike
Josh Burek, Director of Global Communications and Strategy, Harvard Kennedy School Belfer Center
Chris Collins, Co-Founder, First Atlantic Capital
Caitlin Conley, student, Harvard Kennedy School
Mari Dugas, Project Coordinator, Defending Digital Democracy, Harvard Kennedy School Belfer Center
Josh Feinblum, student, Massachusetts Institute of Technology
Siobhan Gorman, Director, Brunswick Group

Stuart Holliday, CEO, Meridian International Center
Dai Lin, student, Harvard Kennedy School
Kent Lucken, Managing Director, Citibank
Katherine Mansted, student, Harvard Kennedy School
Nicco Mele, Director Harvard Kennedy School, Shorenstein Center
Debora Plunkett, former Director of Information Assurance, National Security Agency
Jim Routh, Chief Security Officer, Aetna
Suzanne E. Spaulding, Senior Adviser for Homeland Security, Center for Strategic and International Studies
Matthew Spector, student, Harvard Kennedy School
Alex Stamos, Chief Security Officer, Facebook
Phil Venables, Partner and Chief Operational Risk Officer, Goldman Sachs

Additional Authors and Contributors

Ryan Borkenhagen, IT Director, Democratic Senatorial Campaign Committee
Michael Chenderlin, Chief Digital Officer, Definers Public Affairs
Robert Cohen, Cyber Threat Analyst, K2 Intelligence
Julia Cotrone, Special Assistant, Definers Public Affairs
John Flynn, Chief Information Security Officer, Uber
Daniel Griggs, Founder and CEO, cmdSecurity Inc.
Eben Kaplan, Principal Consultant, CrowdStrike
Greg Kesner, Principal, GDK Consulting
Ryan McGeehan, Member, R10N Security
Jude Meche, Chief Technology Officer, Democratic Senatorial Campaign Committee
Eric Metzger, Founding Partner and Managing Director, cmdSecurity Inc.
Zac Moffatt, CEO, Targeted Victory
Harrison Monsky, student, Harvard Law School
Colin Reed, Senior Vice President, Definers Public Affairs
Jeff Stambolsky, Security Response Analyst, CrowdStrike
Frank White, Independent Communications Consultant
Sally White, student, Harvard University
Rob Witoff, Senior Security Manager, Google

Belfer Center Web and Design Team

Arielle Dworkin, Digital Communications Manager, Harvard Kennedy School Belfer Center
Andrew Facini, Publications and Design Coordinator, Harvard Kennedy School Belfer Center

Downloads

Cybersecurity Campaign Playbook [PDF]

Handout For Staff Members [PDF]

Handout For Family Members [PDF]

For more information on this publication: Please contact the Belfer Communications Office
For Academic Citation: "Cybersecurity Campaign Playbook." Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2017.

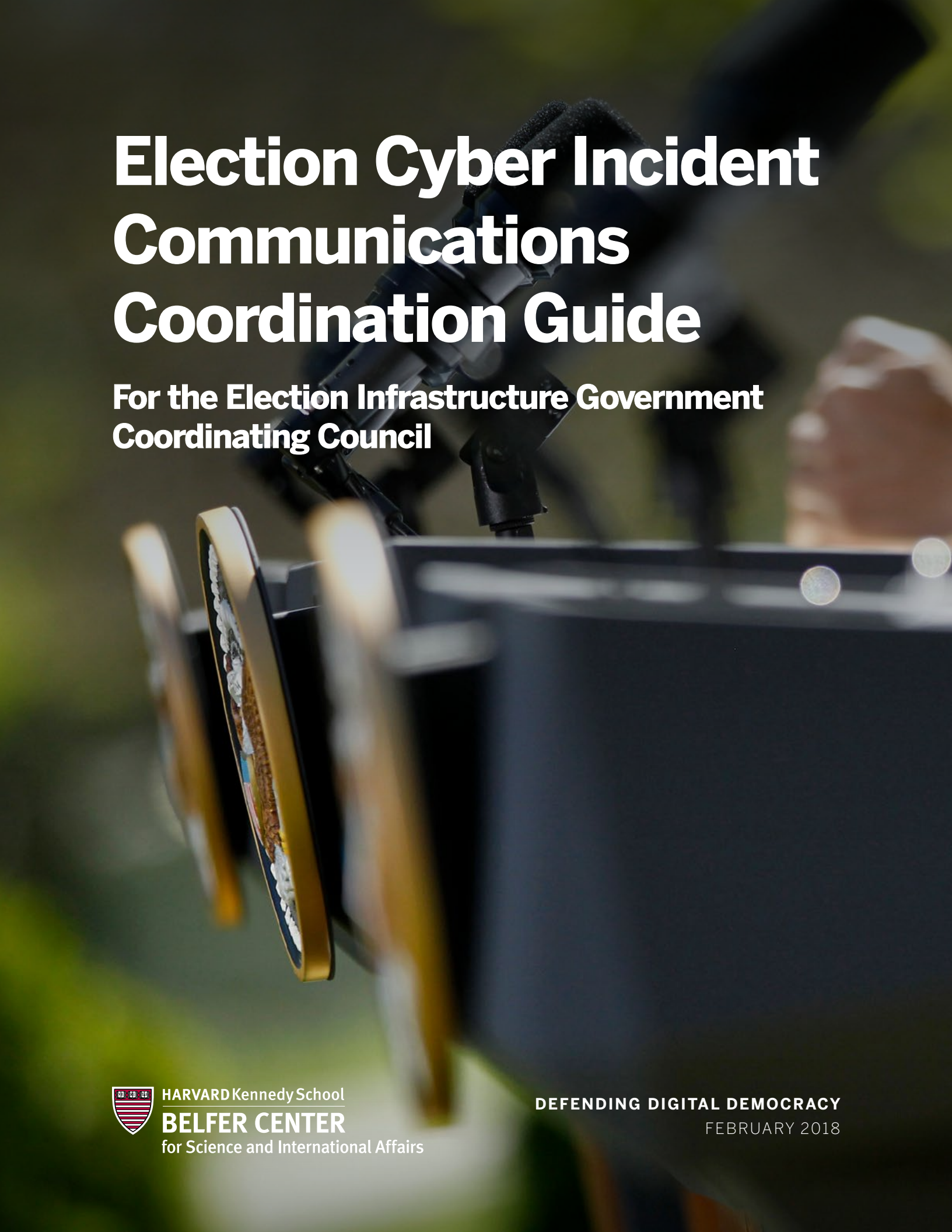
Harvard Kennedy School Belfer Center

Election Cyber Incident Communications Coordination Guide

February 2018

Election Cyber Incident Communications Coordination Guide

For the Election Infrastructure Government Coordinating Council



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Statements and views expressed in this document are solely those of the authors and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Design & Layout by Andrew Facini

Cover photo: A view of the podiums during a news conference in the Rose Garden at the White House, Monday, April 2, 2012. (AP Photo/Charles Dharapak)

Copyright 2018, President and Fellows of Harvard College

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Election Cyber Incident Communications Coordination Guide

For the Election Infrastructure Government Coordinating Council

Contents

Defending Digital Democracy Project: About Us 2
Authors and Contributors 3
Acknowledgments 4
How to Use this Communications Guide 5

Executive Summary and Purpose 6

Strategy, Mission, and Objectives 7

Establishing a Cyber Education Baseline 9

Cyber Crisis Communications Best Practices 11

Planning Ahead 11
Communications Response 12

Communications Process 14

Phase 1: Baseline Communications Activities 15
Phase 2: Communications Planning, Activation, and Coordination 17
Phase 3: Message/Document Drafting, Coordination, and Distribution 22
Phase 4: Evaluation and Feedback 24

Communications Coordination and Response Checklist 26

Conclusion 31

Defending Digital Democracy Project: About Us

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help secure democratic elections against cybersecurity threats and information operations.

There are two groups on the frontlines of defending democracy: (1) political campaigns, which enable citizens to pursue elected office; and (2) election officials, who ensure the election process is free and fair.

Last year, we set out to provide campaign and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections. In November 2017, we released "The Campaign Cybersecurity Playbook" for campaign professionals.

Now, we are releasing a set of three playbooks designed to be used together by election administrators: "**The State and Local Election Cybersecurity Playbook**," "**The Election Cyber Incident Communications Coordination Guide**," and "**The Election Incident Communications Plan Template**." What follows is the Coordination Guide.

D3P is a bipartisan team of cybersecurity and policy experts from the public and private sectors. To better understand the cyber threat and other challenges that election administrators face, our team spent four months interviewing state officials about their communications practices and how they would or would not apply these practices in a cyber incident. We spoke with state and local election officials, as well as key national-level players and members of the Election Infrastructure Government Coordinating Council (EI-GCC).

These interviews exposed the range of challenges election officials confront in the cyber domain. One of the most significant needs we encountered was the ability to communicate consistently across states in the event of a major election cyber incident, in order to maintain public trust.

This Guide is primarily intended for use by the EI-GCC to coordinate multiple voices (and multiple facts) in an election cyber incident that crosses traditional jurisdictions. We are releasing the Guide publicly, because a range of officials may be interested in learning more about how state and local leaders can, and should, coordinate their communications in the event of this type of cyber incident. We hope this Guide becomes a starting point for the EI-GCC to establish its role as a central communications node in the event of an election cyber incident.

Finally, we would like to thank the election officials around the country for whom we wrote this guide You are the frontline defenders of democracy. We hope this effort helps make that tremendous responsibility a little easier.

Good luck,
The D3P Team

Authors and Contributors

This project was made possible by dozens of people who generously volunteered their time. Special thanks are due to **Siobhan Gorman** for leading the project and who, in addition to **Matt Chandler**, **Meredith Davis Tavera**, and **Chris Farley**, wrote this Coordination Guide.

We are also indebted to the people listed below who invested countless hours in reviewing drafts and providing input.

SENIOR ADVISORY GROUP

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Heather Adkins, Dir. of Information Security and Privacy, Google

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Siobhan Gorman, Director, Brunswick Group

Yasmin Green, Head of Research & Development, Jigsaw (Alphabet)

Stuart Holliday, CEO, Meridian International Center

Kent Lucken, Managing Director, Citibank

Debora Plunkett, former Director of Information Assurance, National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Suzanne Spaulding, Senior Advisor for Homeland Security, Center for Strategic and International Studies

Alex Stamos, Chief Security Officer, Facebook

CONTRIBUTORS

Lori Augino, Director of Elections, WA Office of the Sec. of State

Matt Chandler, Partner, Frontier Solutions

Caitlin Conley, Executive Director, D3P

Amy Cohen, Executive Director, National Association of State Election Directors

Meredith Davis Tavera, D3P, Harvard Kennedy School

David Forsey, Policy Analyst, National Governors Association

Shannon Cortez, Deputy Director of Elections, WA Office of the Secretary of State

Chris Farley, Associate, Albright Stonebridge Group

David Forsey, Policy Analyst, National Governors Association

Karen Ejiofor, Staff Assistant, Belfer Center

Siobhan Gorman, Director, Brunswick Group

Eben Kaplan, Principal Consultant, CrowdStrike

Jane Khodos, Senior Director, Comms. and Content, FS-ISAC

Matthew Masterson, Commissioner, Election Assistance Commission

Jeff McLeod, Division Director for Homeland Security and Public Safety, National Governors Association

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

Michelle Tassinari, Director/Legal Counsel, Elections Division, Office of the Secretary of the Commonwealth of MA

BELFER CENTER WEB & DESIGN TEAM

Arielle Dworkin, Digital Communications Manager, Belfer Center

Andrew Facini, Publications and Design Coordinator, Belfer Center

Acknowledgments

The D3P team would like to especially thank Heather Adkins of **Google**, Yasmin Green of **Jigsaw**, the **Hewlett Foundation**, the **Democracy Fund**, and the **Belfer Family**; without whom this Playbook would not have been possible. Additionally, we would like to thank the following organizations and offices for sharing their time with us through conversations, simulation participation, or field visits. Your perspectives were critical in shaping our approach to this document.

Department of Homeland Security (DHS)

National Association of State Election Directors (NASED)

National Association of Secretaries of State (NASS)

National Governors Association (NGA)

National Guard Bureau (NGB)

Election Officials from the Following States and Jurisdictions:

Atlantic County, New Jersey

Nevada County, California

Orange County, California

Santa Clara County, California

State of Colorado

Arapahoe County, Colorado

City and County of Denver, Colorado

State of Connecticut

Escambia County, Florida

Cook County, Illinois

State of Louisiana

State of Maryland

Caroline County, Maryland

Commonwealth of Massachusetts

State of Minnesota

State of Nevada

Clark County, Nevada

State of New Jersey

Mercer County, New Jersey

State of North Carolina

State of Ohio

State of Oregon

Multnomah County, Oregon

Commonwealth of Pennsylvania

State of Rhode Island

State of Tennessee

State of Vermont

Commonwealth of Virginia

State of West Virginia

Harrison County, West Virginia

State of Washington

State of Wisconsin

How to Use this Communications Guide

This communications guide includes best practices and guidelines to help the Election Infrastructre Government Coordinating Council (EI-GCC) quickly coordinate the response to an election-related cyber incident that affects more than one state during the early days of the incident. While every cybersecurity incident is unique, this document provides a foundation on which the EI-GCC can build a response that addresses the incident with the goal of maintaining confidence in the election system.

This Guide should be owned by the communications director, or a similar position, at the EI-GCC and be updated at least annually.

Key topics include:

Strategy, Mission, and Objectives: The purpose of the Guide is to help election officials maintain public confidence in the integrity of the U.S. election system in the event of an election-related cybersecurity incident.

Establishing a Cyber Communications Baseline: This section explains the importance of educating the public and other key stakeholders on cyber threats facing the election process and steps currently being taken to counter them.

Cyber Incident Best Practices: This section includes best practices for communicating with the media and other key stakeholders.

Communications Process Workflow: This component includes diagrams that outline who will manage the cyber crisis communications response and serve as spokesperson during an incident.

Response Checklist: This checklist broadly outlines steps that should be taken during the first several days after learning about a potential incident.

Executive Summary and Purpose

What constitutes a "cyber incident" in elections can range from theft of voter registration data to disruption or manipulation of the vote tally. This Guide is designed to help coordinate and align communications across jurisdictional boundaries in an election-related cybersecurity incident that involves more than one state. Its primary purpose is to maintain (or regain) public confidence in the face of such an incident.

This Guide is written to help the Election Infrastructure Government Coordinating Council (EI-GCC) assist state and local election officials, who will need to communicate across jurisdictions if an election-related cyber event has impacts beyond a single state. While every jurisdiction should have its own plan to respond to a cyber incident, many incidents will have implications beyond state boundaries. It is critical to coordinate the response from the outset, so public comments confidently convey that the issue is being addressed and maintain public trust in election systems across the country.

We recommend the creation of a communications coordination structure within the EI-GCC, including a communications director, or similar role, who would be a key spokesperson in a cyber crisis.

A multistate cyber incident could take many forms. It could be a series of incidents that collectively have a broader impact. It could be one or a few incidents that, because of their strategic significance or other factors, have an impact beyond state boundaries, or receive outsized attention from national media outlets. This could even be a false rumor that requires a coordinated effort to stamp it out.

This Guide provides:

1. A set of best practices for communicating about an election-related cyber incident

2. A process for coordinating multistate communications decision-making, including spokespeople and communications messages

Additional communications response materials, including a sample escalation process and scenario-planning materials, are available to election officials and can be obtained upon request from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.

Strategy, Mission, and Objectives

The potential for cyberattacks on our elections systems is an unfortunate reality of our time. Election officials should recognize, and plan for, a possible incident. **The primary objective of this communications guide is to enable the EI-GCC to help election officials maintain public confidence in the integrity of the U.S. election system** in the event of cyber incidents both locally and crossing state boundaries.

Election officials from both parties and at all levels of government agree that there is a shared national interest in preserving the public trust in our election system.

A central component of maintaining trust is providing the public with timely and accurate information. Equally important is dispelling inaccurate information as quickly as possible, especially in today's perpetual cycle of traditional and social media coverage.

Maintaining public trust is most effectively accomplished when election officials—across parties and jurisdictions—speak with one coordinated voice. If federal officials are contradicting state leaders, as occurred in 2016, the public is left confused and it can become all the more difficult to maintain confidence in the election process. Likewise, if federal, state, or local officials are contradicting one another, it is counterproductive and confusing to the public. For these reasons, EI-GCC will play a crucial role in coordinating the response.

All public statements should demonstrate the incident is being handled competently. Any specifics that are provided should be limited only to those that will not change. The scope of the incident, for example, is likely to shift and shouldn't be discussed publicly at the outset. Modifying your story can undermine confidence in the management of the incident and the election system itself.

To institutionalize a means to maintain public trust, **the communications response strategy underlying this Guide coordinates communications messages and delivery among election officials in a multistate cyber incident** to ensure consistency and accuracy of public information. To enable a unified response, we provide communications best practices and coordination processes.

Elections are governed at the state and local level, and there is a national interest in maintaining the integrity of, and confidence in, our elections system. So it is important to have a process that

will enable officials from all levels of government to: obtain and analyze the information; decide who will speak about the national implications of the incident; and provide information and communications to all elections officials, so they can communicate accurately, dispel rumors, and reinforce coordinated messages.

Beyond the coordinated multistate process outlined in this Guide, election officials at all levels of government should take measures to prepare for a cyber incident.

Among the steps you can take immediately are:

- **Establish (or update) a state or local communications response plan** to an election-related cyber incident. For a template state or local cyber communications plan please see the Election Cyber Incident Communications Plan Template.
- **Ensure that the communications plan is aligned** with the corresponding technical response plan, and that both are regularly updated.
- **Test those plans** with simulations.
- **Obtain regular updates** on cyber threats, particularly as they relate to elections.
- **Maintain relationships with officials** who will be relevant to coordinating a response to any cyber incident, including federal officials at the local level and other local community leaders.
- **Coordinate with political parties.** It is much easier to agree to protocols for sharing information about and responding to a cyber incident before the incident and before an election.
- **Educate the public about the work you are doing.** Set the expectation that there will likely be some cyber threat activity during an election and explain how that activity differs from what would be required to interrupt the elections process.

It is important to update and exercise communications response plans frequently—at least every year—to familiarize new players with the process and ensure you apply lessons learned from past experiences and exercises.

Establishing a Cyber Education Baseline

The public needs to understand the steps state elections officials are taking to counter cyber threats, as well as how difficult it is to execute a cyberattack that will disrupt an election outcome. If the public, and the media, understand the "new-normal," baseline activity of cyber threats targeting elections, they will be less likely to worry unnecessarily about news of small-scale election-related cyber incidents. If you don't have to spend considerable time allaying concerns over inconsequential incidents, you can focus your attention on the consequential ones.

The main point to make is that cyberattacks are now an issue all election officials must contend with, and the states have taken, and continue to take, steps to mitigate those threats. However, not every attempt is successful, and even successful ones are very unlikely to impact the outcome of an election.

Communications in a cyber crisis are most effective when the public has a baseline understanding of:

- The continuing work at all levels of government to counter that malicious activity and try to ensure it does not escalate to a major cyber incident
- The nature of the election data your agency holds, most or all of which is public data
- The malicious, but inconsequential, cyber activity that takes place regularly

We recommend that the EI-GCC consider taking on some of this public education role, which would address issues that extend across the states. The council is in a strong position to draw on data from across the country and across levels of government about both threats and actions being taken to enhance the cyber defenses of election systems. For this reason, we suggest that it consider publishing an annual report on the state of election cybersecurity.

The EI-GCC, perhaps in concert with the relevant associations and Information Sharing and Analysis Centers, could provide a regular cadence of cyber threat information, so the public understands how frequently attempts are made by a range of cyber threat actors to target election

infrastructure. Making this information common knowledge will mitigate the tendency to treat every reported attempted attack as a reason to question the election system.

The type of information you may want to share could include statements such as: "Based on threat information from the Department of Homeland Security and the Federal Bureau of Investigation (or state/local law enforcement), we are taking the following steps to address and mitigate these threats." If appropriate, this effort could take the form of regular background briefings for the media, as well as online materials and public panels or other educational events for other key stakeholders. The EI-GCC could also consider a joint public panel or forum with representatives of both political parties to discuss measures states are taking to mitigate cyberattacks.

The EI-GCC should also consider sharing limited, aggregate information on successful attacks once they have been addressed, which would establish the EI-GCC as a valuable resource for this type of information.

You should couple the cyber threat data with information on the actions states and localities are taking to strengthen the cyber defenses of election systems. This information should be specific enough to be credible while not being so detailed as to undermine your defenses. Work closely with information security and legal experts to strike the right balance.

We discuss how to establish a communications baseline in more detail in the section on communications process on Page 15.

Cyber Crisis Communications Best Practices

Election-related incidents fall broadly into five categories:

- Online rumors that seek to undermine confidence in an election
- Reconnaissance of election-related systems
- Theft of voter or other election data
- Data manipulation that could affect an election outcome
- Data destruction

The top priority in a cyber crisis will be to maintain public trust. The most effective way to achieve that goal is to respond confidently and quickly. To do this, the EI-GCC will need to prepare, train for, and test its response ahead of time—especially because it is a new organization.

Planning Ahead

Near-term Planning	Longer-term Planning
• **Determine internal roles and responsibilities**. Make sure there is a clear escalation process for the EI-GCC and the right teams are talking to each other in the event of a cyber incident. Make an individual responsible for ensuring that this process is established and updated. • **Assess the current crisis communications plan** and analyze communications gaps and weaknesses. • **Plan your response to a cyber crisis in advance** with a communications plan, including a decision-making protocol and communications materials. • **Ensure that cyber incident response is part of the operational continuity plan**. Make sure there is a backup communications plan and system in place.	• **Conduct crisis simulation and table-top exercises**, coordinated with legal, technical, and outside advisors, including key senior leaders from multiple states, counties, coordinating bodies, and the federal government. • **Conduct stakeholder mapping and a risk analysis** to understand risks to trust in the election system, priority stakeholders, and how to reach stakeholders to address key concerns. Pay particular attention to outreach to voters and political parties. • **Educate the media** through background meetings and public events on the resiliency of the election system, and the current work to mitigate cyber threats. • **Educate the public** through online channels and public events on the resiliency of the election system and the current work to mitigate cyber threats.

Communications Response

Best Practices

Be transparent but careful. Transparent communication builds trust, but in a cyber incident, you will have few facts at hand, especially at the outset. Public comments should demonstrate that you are taking the issue seriously, but avoid providing any details that may change as the investigation progresses, so you don't have to correct yourself down the line. Avoid speculation on the perpetrator of the incident.

Focus on actions you are taking to address the issue. To demonstrate that you are taking the issue seriously, you should talk about the steps you are taking to protect voter information and address any broader risks to the system.

Provide context. In an election-system incident, there will be a temptation for public speculation. Counter speculation with facts and context to reduce the risk of undermining public trust. Include metrics whenever possible.

Be visual. Cybersecurity can be challenging to understand depending on a person's technical background. The quickest way to get your message out is to pair it with a graphic. Connect with design teams who can provide you infographics and develop a library of graphics and photos you can draw from.

Use the right digital tools. Use social media to dispel rumors. When a cyber incident strikes, social media is now a go-to source of immediate information. In practice, this means using it selectively to counter misinformation and inaccuracies.

Learn from the incident. Use your and others' experiences to improve your cybersecurity practices and crisis plans.

Guidelines for Communicating with the Public

Focus your communications on your most important stakeholder—the public. You will be tempted to discuss the components of the incident. Instead, talk about what you are doing to address public needs or concerns in this given situation.

Speak plainly. Cybersecurity can be off-putting to nontechnical audiences. Use anecdotes and examples to demystify cybersecurity issues whenever possible.

Demonstrate transparency by communicating with the public on a regular basis. Establish a regular series of communications with the media and the public about the cybersecurity measures you are taking now, so that the first time they hear from you is not in a crisis.

Best Practices for Countering Misinformation

Establish the facts, and double-check them. You need to ensure that you are operating from a factual position before countering misinformation, so check your facts with multiple sources before citing them publicly. Ask all appropriate questions and put in the work before you speak to be certain that you do not accidentally provide misleading information.

Develop a simple, accurate, short counter-message. Develop a clear statement that contains only the facts. Avoid complex messages. You can provide additional nuance later.

Respond quickly. Misinformation can spread rapidly through social media and broadcast commentary. Your counter-message should be ready to disseminate as soon as possible.

Be transparent. Caveated, incomplete, or "no comment" responses can fuel conspiracy theories by making it appear your organization has something to hide. Demonstrating transparency can help to counter false claims. Opportunities to demonstrate transparency could include inviting reporters "behind the scenes" at a polling place.

Engage on all platforms. Misinformation can spread across multiple platforms, including social media and traditional media. To counter misinformation, deliver a clear, factual message on all available platforms.

Avoid repeating misinformation. Focus on providing accurate facts and do not repeat the false messages. For example, if false rumors circulate that lines at the polls are many hours long, avoid saying that rumors of long lines are circulating. Instead, your message should be that lines are short and moving quickly.

Communications Process

Maintaining a coordinated process is critical to effective and efficient communications planning and response to a cyber-related incident. For an incident affecting multiple states, this coordinated communications process outlines:

- Key stakeholders
- Phased planning and response
- Coordination functions
- Feedback loop to incorporate lessons learned

In this communications process, we assume that information and messaging coordination functions will be performed by cross-jurisdictional organizations that have played a similar role in past crises. Further, we recommend that new coordinating functions and mechanisms be created to execute information-sharing and communications.

We recommend that the EI-GCC—with support from other interested parties, such as the National Association of Secretaries of State (NASS), International Association of Government Officials (IGO), the U.S. Election Assistance Commission (EAC), the National Association of State Election Directors (NASED), and the National Governors Association (NGA)—establish a Cybersecurity Communications Response Group (CCRG).

This newly formed entity will provide the EI-GCC and its stakeholders with a communications coordination function that currently does not exist, allowing for collaborative, coordinated public message planning and execution if and when it is needed in the future.

Phase 1: Baseline Communications Activities

On a regular basis, the CCRG will provide updates to the public and other key stakeholders on current cyber threats and actions being taken to counter them. These baseline updates, whether part of a regular cadence or spurred by suspected nefarious activity, should be developed and coordinated with the expectation that they will be made public. Audiences and stakeholders are catalogued below with recommendations for actions that can be taken now to establish or maintain relationships with them.

Communicating with these groups on a regular basis, before something happens, is key to setting a baseline with critical audiences so that there is a level of understanding around the issue that allows mutual alignment on escalation and coordinated response. In order to provide this ongoing education, we recommend communicating early and often, in addition to when moments of interest (i.e., elections) arise. This baseline work could take the form of behind-the-scenes demonstrations and briefings for your audiences.

Stakeholders may include:

State / Local Comms. Counterparts

Law Enforcement

Federal / State Lawmakers

Media

Interested Parties

State and Local Communications Counterparts: Knowing your state and local counterparts is key to the planning and response actions discussed in later phases. The EI-GCC should maintain a "living list" of communications officials and accurate contact information, so these individuals can be reached on short notice for incident coordination and planning.

Law Enforcement: In the event of a cyber incident, federal, state, and/or local law enforcement will be involved in the response. Creating and maintaining relationships with key law enforcement officials and associated communicators in law enforcement agencies ensures more seamless coordination and information-sharing before, during, and after an incident.

Federal/State Lawmakers: Federal and state lawmakers play an important role in authorizing and overseeing election and cybersecurity measures. They also are likely to speak publicly about an election-related cyber incident, so communication with them is

critical before, during, and after an incident. Not only are lawmakers beneficiaries of a safe and secure elections system, but they have a vested interest in maintaining the public's trust in that system. Communicators should build relationships with key figures in Congress and statehouses, including their respective communications staffs, in advance.

Media: The media is a key information conduit to voters, providing news and commentary that shapes and defines public opinion and a belief in the election system's integrity. Establishing ongoing relationships with key reporters who cover both cybersecurity and election-related issues at the national, state, and local level will be important in shaping accurate coverage throughout all phases of cyber-related preparation and response.
You should focus on two categories of media:

Traditional Media—Mainstream outlets and reporters;

Influencer Media—This category includes influential bloggers, outlets, and commentators, as well as outlets likely to reach them.

Interested Parties: You should develop relationships with voting advocacy and other third-party groups, because they play a role in maintaining the public's confidence in elections. Political parties an campaigns are a critical group with which you should develop a trusted relationship in advance. Third-party groups may also include vendors, researchers specializing in elections, technology service providers, or other industry service providers. We recommend as a next step that the CCRG develop an initial list of key groups, which should be maintained and updated by the team lead.
This list could include:

Political Parties and Campaigns

Election Groups

Think Tanks

Academics

Phase 2: Communications Planning, Activation, and Coordination

Cyber-related incidents rely on evolving investigations, making their scope and impact difficult to understand, particularly at the outset. This can make communications decision-making, coordination, and messaging even more important for reducing confusion.

Some incidents may be discovered as an attack or breach occurs, while most tend to be discovered after the fact—often after significant time has passed. The key to an effective response is not just coordination but also knowing with whom to coordinate. In any response, there are likely to be multiple voices speaking publicly, at both the national or field level.

In this phase, we assume an anomalous event has been identified, which activates a communications coordination scheme. It may be detected by a range of entities, such as a security researcher, state/local election official, law enforcement, or media.

When an incident occurs, many representatives from a variety of organizations will become involved. The section below outlines resources, coordination mechanisms, lines of coordination, and a checklist to be used in response to, or in advance of, a cyber-related incident.

Assembling Key Players

Note: *The U.S. Federal Government's National Response Framework outlines public information as an Emergency Support Function (ESF) and includes a framework for public information coordination and action around incidents that involve, or may involve, federal response. This process aligns with the ESF #15 Standard Operating Procedure.*

CCRG Roles & Responsibilities: The CCRG should establish the following roles for responding to a multistate cyber incident. These individual roles can be filled by specific people from a variety of interested parties, which may include, but are not limited to, NASS, NASED, IGO, EAC, and NGA.

Please note that as the EI-GCC builds on this Guide, updates should include a table with these roles assigned to individuals, along with their contact information.

Communications Director–On behalf of the EI-GCC, oversees the functional coordination resources, processes, and staff. Is responsible for overall operational direction and communications messaging development in cooperation and coordination with EI-GCC and interested parties. The communications director position can be filled by different people on a rotating basis; for example, the EI-GCC could designate a communications director to stand duty quarterly. The role should be filled by a senior communicator from the EI-GCC participants or other interested parties and have the relevant management, crisis, and media operations experience to understand not only their role but also the other roles outlined as part of the CCRG.

Affected Community Communications Representatives–Usually senior communicators from affected state or local jurisdictions representing a "field" perspective and providing relevant incident-related information to the coordination process. This may include a communicator from the governor's office and/or communicators from state and/or local elections offices.

Media Operations Director–Responsible for communication with reporters and for media monitoring on behalf of a multi-state communications coordinating body. Oversees near-term, "24-hour" communication operations, i.e., execution of communication plans.

Social Media Director–Responsible for online communications via ESCC web platforms, as well as coordination with interested parties' digital media teams in order to promote and cross-promote content.

Communication Plans Director–Responsible for forward-looking communication plans beyond the immediate "24-hour" period.

Congressional/Inter-governmental Affairs Liaison–Responsible for coordinating congressional/governmental briefings for members of Congress, state legislatures, or other elected officials with communications staff. Coordinate through the Affected Community Communications Representative, who is likely to be a member of the ESCC or interested parties' government affairs team.

Law Enforcement Affairs Liaison–Responsible for coordinating communications information with law enforcement and affiliated communicators.

Technical Liaison–Responsible for being the conduit of technical information between operational and communications teams. Ensures accuracy of technical data being released by communications team and serves as subject-matter expert for all such information.

Activation of the CCRG: The CCRG, while regularly communicating in Phase 1 during baseline operations, should plan for and exercise the activation of the CCRG in a crisis. Activation of the CCRG would be at the discretion of the Communications Director, with input from operational leads in response to a verified or potential incident. Additional information on the escalation process is in the Appendix available to election officials and can be obtained upon request from NASS, NASED, or the EAC

Generally speaking, this activation would be executed via a blast email to CCRG members with shareable background information on the incident, direction on the use of coordination mechanisms (discussed below), and next steps. For example, on discovery of a potential incident, the Communications Director would activate the CCRG by hosting an Election Sector Incident Communications Coordination Line call regarding the incident, thereby beginning the communications coordination process.

Election Sector Incident Communications Coordination Line (ESICCL): This bridge line is a standing conference call line that can be created to use for coordination before, during, or after a cyber-related incident. The CCRG will maintain a list of relevant contacts from federal, state, and local election offices in order to invite relevant parties to a call, should it be necessary. This resource does not currently exist and it would be incumbent upon the CCRG to coordinate the creation of this standing line at the outset.

Election Sector Information Center (ESIC): In the event of a multistate event, the CCRG should create a specific Information Center where communications activity is planned, coordinated, and executed real-time. This should include all the roles above and can reside in one physical location or it could be done virtually through online means. An ESIC would be the functional nerve center of all communications-related activity.

Using the Election Sector Incident Communications Coordination Line (ESICCL)

As the standing conference call line for election sector cyber-related incidents, the ESICCL can be a key coordination mechanism for communicators to share both operational data, as well as coordinate messaging and communications-related activity.

Upon the activation of the CCRG, the Communications Director will stand up the ESICCL and distribute the time and conference line to invited participants for an initial conference call. This call could include representatives from affected communities, as well as the CCRG roles listed above and any other CCRG participants or outside advisors with relevant subject-matter expertise.

The call agenda can follow a regular rhythm:

- Roll call
- Opening remarks by Communications Director for CCRG
- Brief operations summary (on-scene reps or operations)
- Summary of major communications plans and events
- Invitee comments
- Messaging coordination requirements outlined by EI-GCC Representative
- Conclusion and next steps

Standing up the ESIC

Should an event rise to the level where ongoing, real-time coordinated public information flow is necessary, the CRCG could stand up either an in-person or virtual ESIC where personnel could work together.

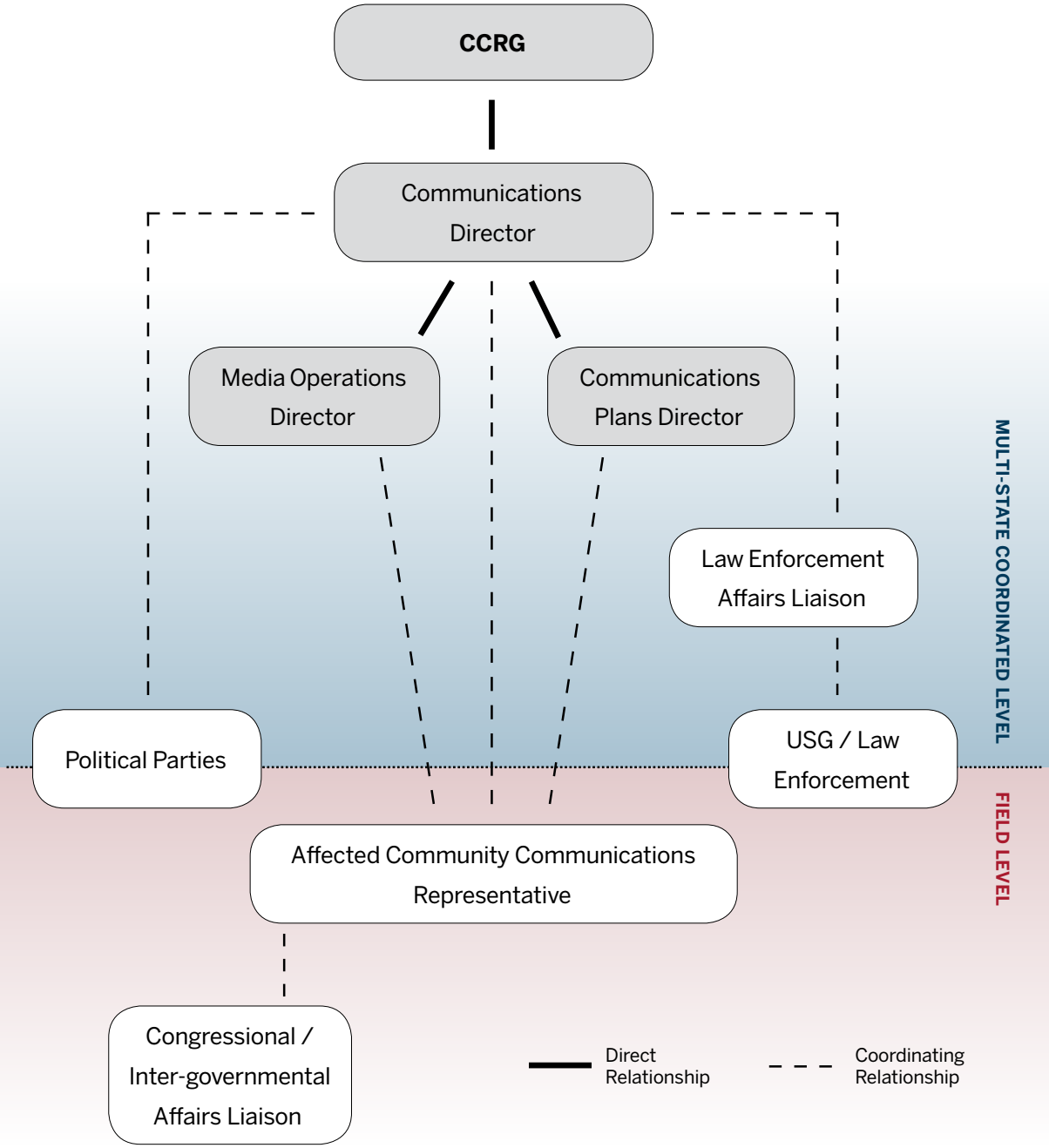
The ESIC would be stood up by the Communications Director, who would make a determination as to the critical personnel needed, as well as the location/online.

The CRCG, as part of steady-state planning, should identify both likely and convenient physical locations where an ESIC could reside should it be needed, as well as functional online collaboration tools to use in the event of a remote ESIC. In general, it is advisable to co-locate the ESIC with any space that is being used to coordinate operational response activity.

Current Coordination Processes

Should there be current coordination processes that are effective in sharing information, such as regular calls or email listservs, continue to use them–particularly prior to, or during the beginning phases of, activation. However, the scope and volume of an incident may make more direct communications, such as via the ESICCL or ESIC, more useful.

Lines of Coordination

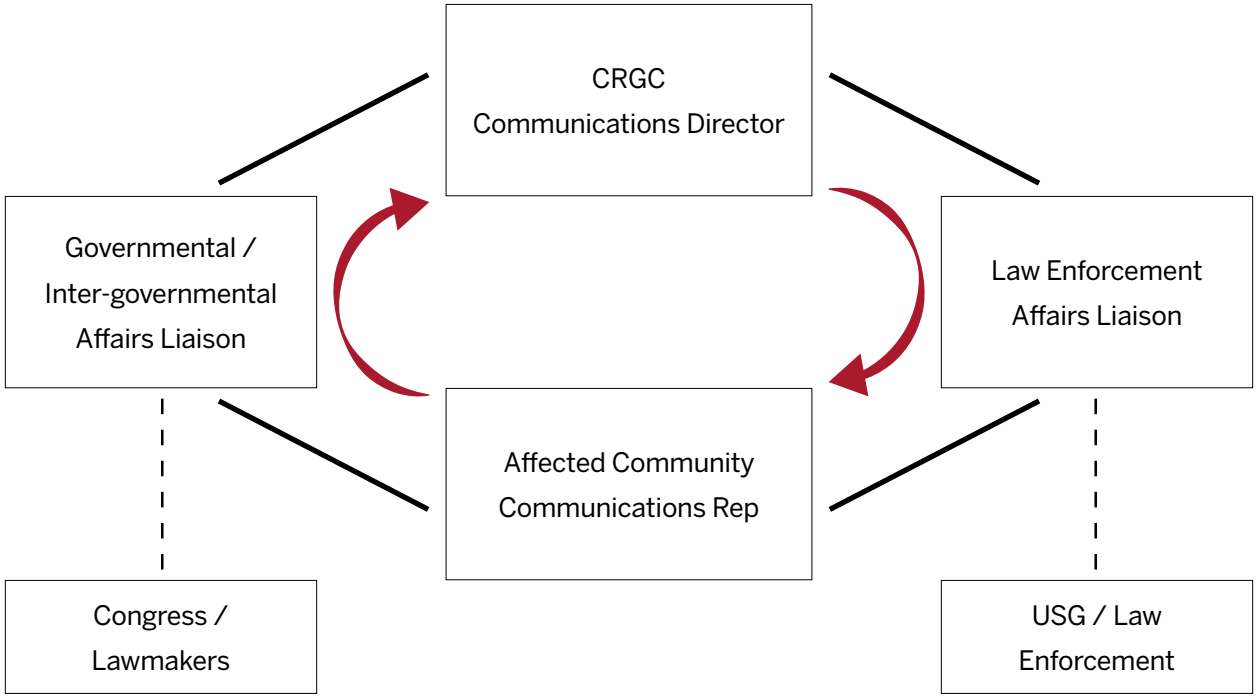


Phase 3: Message/Document Drafting, Coordination, and Distribution

Message/Document Drafting and Coordination

It is best to have some communications materials ahead of time; however, every incident is different and depends on a range of factors, so communicators will oftentimes have to adapt on the fly.

Messaging will need to be adapted, drafted, coordinated, and distributed quickly in order to effectively respond. In addition to the coordination resources, mechanisms, and processes described above, the diagram below shows how that loop may work practically, in and among the various parties who will be speaking publicly.

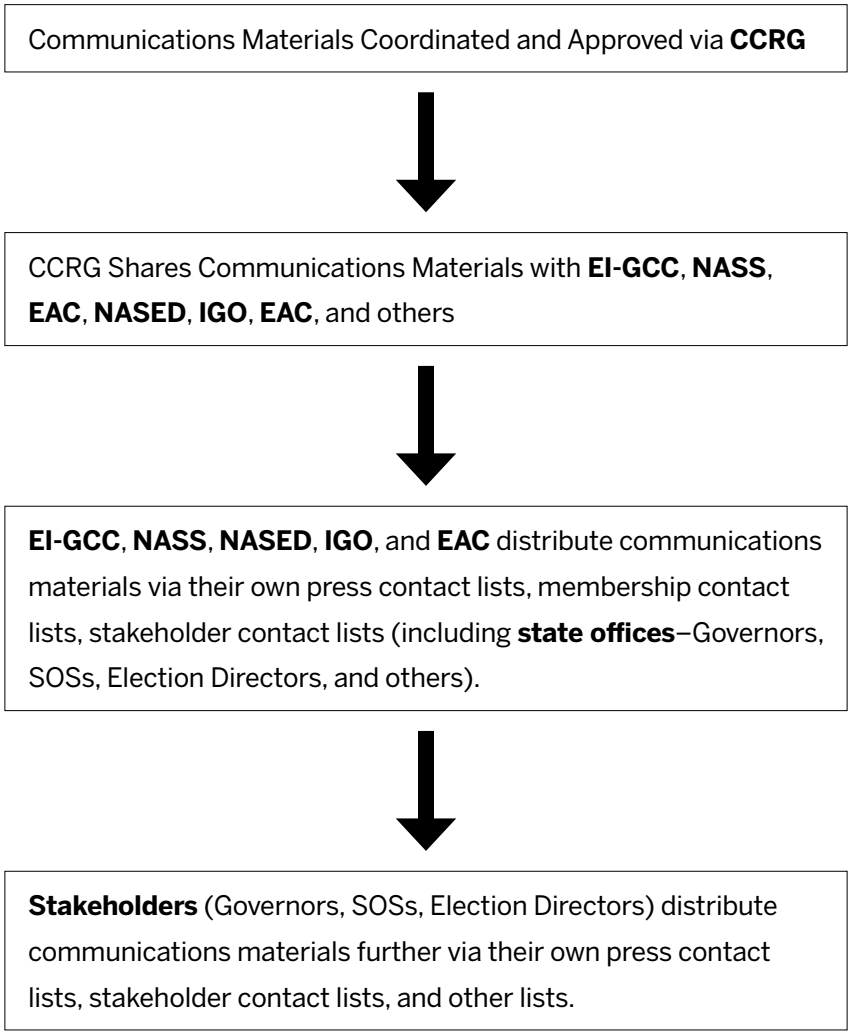


The CCRG staff will not necessarily retain authority to approve messages emanating from affected communities' communications staffs, nor vice versa; however, the CCRG staff can provide message guidance when needed or warranted. In addition, key inputs should be sought from Congressional/Inter-governmental Affairs and Law Enforcement Liaisons, and approval authority can be retained by those communicators with whom these liaisons work at their home agencies or organizations.

Distribution

Distribution of approved communications materials to the public and other stakeholders should leverage, and mirror, existing processes to the degree possible. The CCRG, by virtue of its makeup, with communications professionals from a variety of relevant organizations, should coordinate the messaging, but largely leave distribution to the organizational members.

A sample distribution process is illustrated below:



Phase 4: Evaluation and Feedback

Incorporating both real-time evaluation and feedback, as well as post-incident after-action reviews into your response is critical to both the response you are currently managing, and capturing lessons learned for the future.

Real-Time Evaluation

While capabilities and resources may differ greatly among affected communities, the CCRG could augment these by providing services that can assist the holistic communications response, including:

> **Media Monitoring**–It is critical to understand how the media tone is shaping up. Media monitoring should be compiled at least daily, providing insight on tone and volume and identifying areas for further concentration or strategic/tactical communications changes.

> **Social Media Analysis**–Similar to traditional media monitoring, social media listening tools and analysis can provide key insight into which messengers are driving conversation about the incident, as well as how voters are reacting to news and sharing information.

> **Call Center Analysis**–If the affected community has a voter call center, it is important to track and analyze the questions and comments received. This information can be a key indicator of misinformation or provide insight into where efforts need to be expanded to get accurate information to voters.

> **Polling/Public Opinion Research**–In order to gain more in-depth insights, polling or public opinion research can do much in terms of uncovering voter reactions to an election-related cyber incident, helping shape near and longer-term strategy.

After-Action Review and Report

Once an incident has concluded, it is important to review communications-related activities, discuss what worked and didn't work, and document those lessons to be incorporated into both steady-state and crisis planning.

Many of the coordination resources and mechanisms described above can be adapted for this purpose, for example the ESICCL call. The after-action process should analyze the incident from start to finish, examining the Plan-Prepare-Respond-Recover communications lifecycle of that incident.

Your after-action report should include:

- A summary of the incident;
- an overview of the operational response;
- the communications objectives;
- and by phase, with specificity:
  - concern
  - outcome
  - recommendations

This after-action process will assist in building your communications response capability and coordination in a resilient process that can be more effectively utilized when facing future incidents.

Communications Coordination and Response Checklist

This checklist will help guide actions prior to, and through, the first several days of a multi-state election-related cyber incident.

There are five lists:

- **Before a cyber crisis**
- **Before a cyber crisis becomes public**
- **Multistate Election-Related Cyber Incident Assessment & Activation**
- **Coordination/Communications Outreach**
- **Products**

Before a cyber crisis

- ☐ Identify office protocol and a crisis communications team. (Should include IT).
- ☐ Create a list of terms with common nomenclature for use by all stakeholders.
- ☐ Set an internal communication plan with elections staff. (How often, when, and where will all staff meet? Information must travel up and down the chain of command with clear boundaries for disseminating information and interfacing with the public/media.)
- ☐ Ensure that all stakeholders can be reached in a crisis without access to networks or smart phones.
- ☐ Craft communications materials that can be used in a potential cyber incident. (For examples, elections officials may request sample materials from NASS, NASED, or the EAC.)
- ☐ Ensure that staff understand their role in a cyber incident. For those who do not have a specific role, ensure they understand why their work matters to the outside world and how they can continue doing their jobs while designated managers handle the cyber incident.
- ☐ Ensure that communications plans can be accessed and are regularly updated.

Before a cyber crisis becomes public

- ☐ Obtain technical briefing. (Assess and verify all information.)
- ☐ Decide whether to activate CCRG.
- ☐ Decide whether website can remain online. If you must disable it, launch a microsite (hosted on a different network) in its place.
- ☐ If email is potentially compromised, use an outside communications channel.
- ☐ Consult authorities, if needed.
- ☐ Meet internally in war room; set internal communication schedule.
- ☐ Determine CCRG roles and responsibilities, if you have not done so already.
- ☐ Assess stakeholders.
- ☐ Determine broad communications strategy.
- ☐ Prepare holding statement.
- ☐ Develop communications plan.
- ☐ Draft additional communications required to execute plan, including a communications rollout plan (includes communication with media, stakeholders, and employees).
- ☐ Establish plan for traditional and social media monitoring.
- ☐ Establish media response protocol.
- ☐ Notify affected employees, if necessary. It may be that only a small group of employees are informed initially. Communicate internally, as needed.
- ☐ Notify stakeholders (See list on reverse page), if appropriate, and galvanize support.

Multistate Election-Related Cyber Incident Assessment & Activation

- ☐ Notification to, and activation by CRCG, of a cyber-related incident or threat.
- ☐ Situation Assessment/Escalation.
  - ☐ **High-Intensity Incident**: Cyber-related incident that triggers reporting obligations, or one that is highly visible requiring response.
  - ☐ **Medium-Intensity Incident**: Cyber-related incident resulting in the loss or compromise of the data or systems, but no formal reporting obligations are triggered. There may be some awareness of the incident, however, spurring proactive communication.
  - ☐ **Low-Intensity Incident**: Cyber-related incident resulting in minor disruptions that may not be visible to public.
- ☐ If Major or Moderate, Media Operations Director and Communication Plans Director identified by Communications Director.
- ☐ Additional Relevant Personnel identified.
- ☐ Contact information for Relevant Personnel distributed.
- ☐ CRCG designates spokesperson, if applicable.
- ☐ Depending on assessment of situation, key messages determined based on specific scenario.

Coordination/Communications Outreach

- ☐ Communications Director activates ESICCL call.
- ☐ Incident Overview.
- ☐ Affected Communities Communications Representative Update.
- ☐ Initial Response Communications Plan.
  - ☐ Designate spokesperson based on type of incident, geography(ies) affected, and scope. In a Major Incident, the spokesperson role may include several people including a EI-GCC representative as well as an Affected Community spokesperson as well to share information at both a field and national level. In a Minor Incident, a single spokesperson may suffice, i.e. an Affected Community spokesperson.
  - ☐ Prep designated spokesperson for media engagement. This includes review of relevant facts and messaging as well as a peer review session, known as a "murder-board."
- ☐ Congressional/Inter-governmental Affairs Update.
- ☐ Congressional/Inter-governmental Affairs activity and plans.
- ☐ Law Enforcement Liaison Update.
- ☐ Law Enforcement Liaison activity and plans.
- ☐ Messaging Coordination outlined by Communications Director.
- ☐ Battle Rhythm (Daily Schedule).
- ☐ Conclusion & Next Steps.
- ☐ Communications Distribution & Rollout.
- ☐ ESIC activation, if necessary.

Products

- ☐ Staffing Plan with updates for Communications Director.
- ☐ Battle Rhythm (Daily Schedule).
- ☐ Staffing Matrix and Organization Chart.
- ☐ Communications Plan.
- ☐ Advisories.
- ☐ Press Releases.
- ☐ Traditional and Social Media Monitoring Reports.
- ☐ Regular/Daily update on response activities.
- ☐ Blog and Social Listening Updates.
- ☐ Talking Points.
- ☐ Website updates.
- ☐ Congressional/Inter-governmental Advisories, fact sheets, operations reports and briefing materials.
- ☐ Daily Communication Summary to include next day activity plans.

Conclusion

As we head into the next election cycle, we hope that this Guide provides additional tools to help the EI-GCC, and by extension election officials across the country, prepare for, and manage, this emerging and evolving cyber risk. As with all communications plans, we recommend that this one be regularly updated by the EI-GCC, as the council further develops and defines its role.

More information is available on different types of communications materials for responding to a cyber incident. Election officials seeking examples of these additional materials can request the communications materials appendix to this document from NASS, NASED, or the EAC.

Do you see a way to make this Playbook better?

Are there new technologies or vulnerabilities we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #electionplaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Copyright 2018, President and Fellows of Harvard College

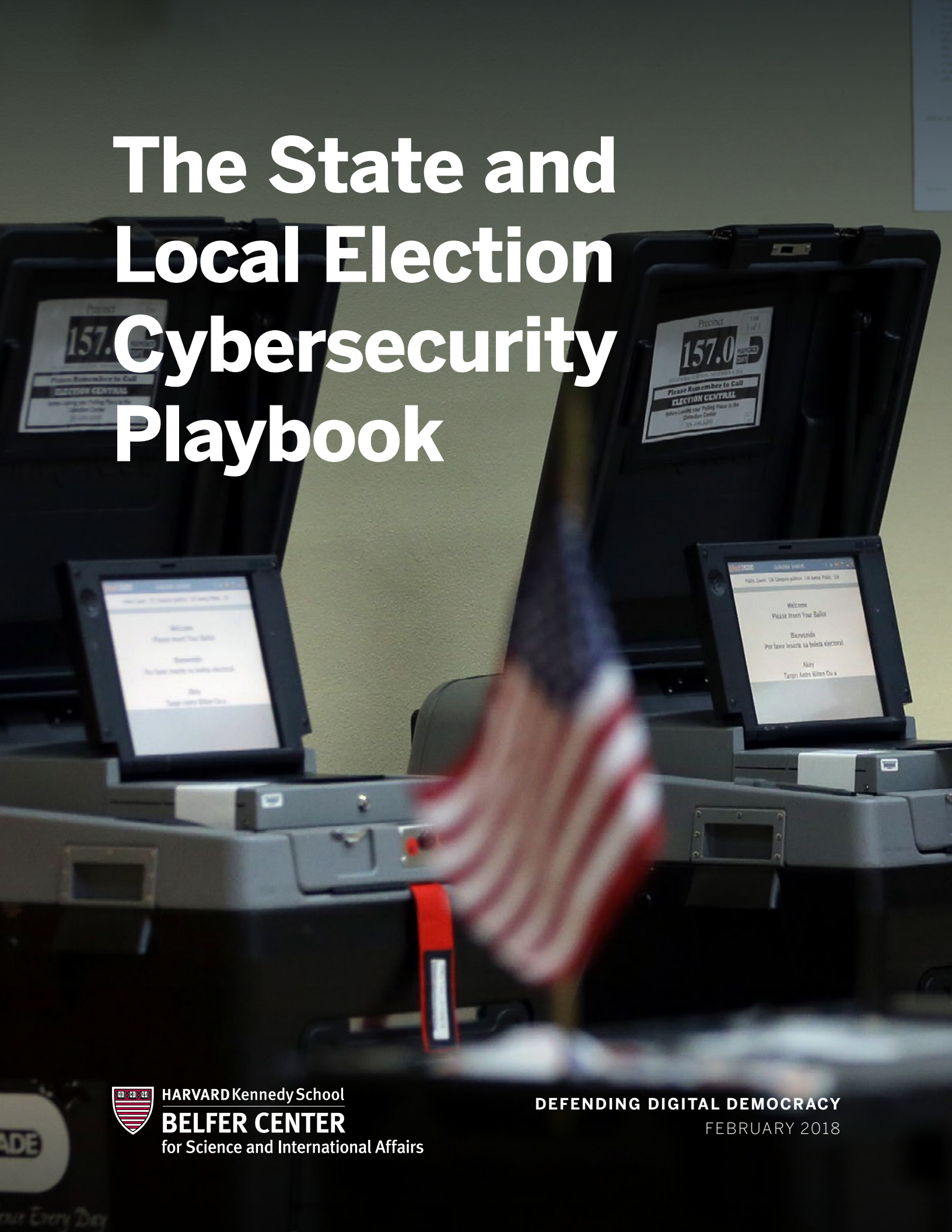
Illustration icons from the Noto Emoji project, licensed under Apache 2.0.

Harvard Kennedy School Belfer Center

The State and Local Election Cybersecurity Playbook

February 2018

The State and Local Election Cybersecurity Playbook



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY

FEBRUARY 2018

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Statements and views expressed in this document are solely those of the authors and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Design & Layout by Andrew Facini

Figure Illustrations by Jordan D'Amato

Cover photo: Voting machines in Miami Shores, Fla., Nov. 8, 2016, (AP Photo/Lynne Sladky)

Copyright 2018, President and Fellows of Harvard College

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

The State and Local Election Cybersecurity Playbook

Contents

Defending Digital Democracy Project: About Us 2
Authors and Contributors 3
Acknowledgments 4

The Playbook Approach 5

Introduction 7

Background 8
- What's at Stake 8
- Cybersecurity Threats to Elections 8

Common Ground 14
- 10 Best Practices that Apply to all Election Jurisdictions 14
- Security Insights by Election System 19

Technical Recommendations 21
- Securing State Election Systems 21
- Voter Registration Databases and e-Pollbooks 22
- Vote casting devices 32
- Election Night Reporting (ENR) 40
- Internal and Public-facing Communications 43

Appendices 49
- Appendix 1. Vendor Selection and Management 49
- Appendix 2. Election Audits 52

External Resources Guide 55

Election Staffer Handout 57

Glossary 59

Defending Digital Democracy Project: About Us

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help defend democratic elections from cyber attacks and information operations.

There are two groups on the frontlines of defending democracy: (1) political campaigns, which enable citizens to pursue elected office; and (2) election officials, who ensure the election process is free and fair. Last year, we set out to provide campaign and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections. In November 2017, we released "The Campaign Cybersecurity Playbook" for campaign professionals. Now, in February 2018, we are releasing a set of three guides designed to be used together by election administrators: "**The State and Local Election Cybersecurity Playbook**," "**The Election Cyber Incident Communications Coordination Guide**," and "**The Election Incident Communications Plan Template**." What follows is The State and Local Election Cybersecurity Playbook.

D3P is a bipartisan team of cybersecurity, political, and policy experts from the public and private sectors. To better understand both the cybersecurity and other challenges that elections face, our team of nearly three dozen professionals spent six months researching state and local election processes. We visited with 34 state and local election offices, observed the November 2017 elections in three states, and interviewed leading academic experts, election equipment manufacturers, and representatives of federal government agencies. We conducted a nationwide security survey with 37 participating states and territories, which identified detailed nuances in election processes and their corresponding risk considerations. We hosted two state election cybersecurity conferences where we engaged state and local election officials in "tabletop exercise" election simulations to increase awareness of the cybersecurity threats they face and improve their ability to mitigate those threats.

This research taught us many things. Most importantly, we learned how difficult it is to defend the multifaceted nature of the elections process. In the United States, elections are among the most complex and decentralized operations in either the public or private sectors. Every state and locality is unique. We were humbled by the intricacies of election operations in each state we visited, and inspired by election officials' incredible level of commitment to the democratic process. We also learned that the leadership of election officials is critical in creating a more secure system. Secretaries of state, election board members, state election directors, and local election administrators set the tone—it's ultimately their job to create a culture in which all staff make security a top priority.

This Playbook is intended for leaders at every level who play a role in running elections. While the future threats elections face are multifaceted, one principle stands clear: defending democracy depends on proactive leadership. This Playbook focuses on the U.S. experience, but it is also relevant to election officials around the world facing similar threats. We have designed it to identify risks and offer actionable solutions that will empower state and local election officials to protect democracy from those who seek to do it harm.

Finally, we would like to thank the election officials around the country for whom we wrote this guide. You are the frontline defenders of democracy. We hope this effort helps make that tremendous responsibility a little easier.

Good luck,
The D3P Team

Authors and Contributors

AUTHORS

Meredith Berger, D3P, Harvard Kennedy School

Charles Chretien, Software Engineer, Jigsaw (Alphabet)

Caitlin Conley, Executive Director, D3P

Jordan D'Amato, D3P, Harvard Kennedy School

Meredith Davis Tavera, D3P, Harvard Kennedy School

Corinna Fehst, D3P, Harvard Kennedy School

Josh Feinblum, Chief Security Officer, DigitalOcean

Kunal Kothari, D3P, Harvard Kennedy School

Alexander Krey, D3P, Harvard Kennedy School

Richard Kuzma, D3P, Harvard Kennedy School

Ryan Macias, Election Assistance Commission

Katherine Mansted, D3P, Harvard Kennedy School

Henry Miller, D3P, Brown University

Jennifer Nam, D3P, Harvard Kennedy School

Zara Perumal, D3P, Massachusetts Institute of Technology

Jonathan Pevarnek, Software Engineer, Jigsaw (Alphabet)

Anu Saha, D3P, Massachusetts Institute of Technology

Mike Specter, D3P, Massachusetts Institute of Technology

Sarah Starr, D3P, Harvard Kennedy School

SENIOR ADVISORY GROUP

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Heather Adkins, Dir. of Information Security and Privacy, Google

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Siobhan Gorman, Director, Brunswick Group

Yasmin Green, Head of Research & Development, Jigsaw (Alphabet)

Stuart Holliday, CEO, Meridian International Center

Kent Lucken, Managing Director, Citibank

Debora Plunkett, former Director of Information Assurance,
National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Suzanne Spaulding, Senior Advisor for Homeland Security,
Center for Strategic and International Studies

Alex Stamos, Chief Security Officer, Facebook

CONTRIBUTORS

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Arjun Bisen, D3P, Harvard Kennedy School

Drew Bagley, Sr. Privacy Counsel & Director of Global Cyber Policy,
CrowdStrike

Daniel Bartlett, D3P, Harvard Kennedy School

Judd Choate, Colorado Election Director and President, National
Association of State Election Directors

Amy Cohen, Exec. Director, National Association of State Election Directors

Mari Dugas, Project Coordinator, D3P

Alan Farley, Administrator, Rutherford County, Tenn. Election Commission

David Forscey, Policy Analyst, National Governors Association

Robert Giles, Director, New Jersey Division of Elections

Mike Gillen, D3P, Harvard Kennedy School

Chad Hansen, Senior Software Engineer, Jigsaw (Alphabet)

Eben Kaplan, Principal Consultant, CrowdStrike

Matt Masterson, Commissioner, Election Assistance Commission

Sean McCloskey, Election Task Force, Department of Homeland Security

Amber McReynolds, Director of Elections, City and County of Denver, Colo.

Joel Mehler, Senior Consultant, CrowdStrike

Robby Mook, Co-Director, D3P

Rachel Neasham, D3P, LoLa

Daniel Perumal, D3P

Debora Plunkett, former Director of Information Assurance,
National Security Agency

Sean Quirk, D3P, Harvard Kennedy School

Matt Rhoades, Co-Director, D3P

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

John Sarapata, Head of Engineering, Jigsaw (Alphabet)

Johanna Shelton, Director, Public Policy, Google LLC

Reed Southard, D3P, Harvard Kennedy School

Suzanne Spaulding, Senior Advisor for Homeland Security,
Center for Strategic and International Studies

Charles Stewart III, Professor, MIT

Michelle K. Tassinari, Director/Legal Counsel, Elections Division, Office
of the Secretary of the Commonwealth of Massachusetts

Frank White, Independent Communications Consultant

BELFER CENTER WEB & DESIGN TEAM

Arielle Dworkin, Digital Communications Manager,
Belfer Center

Andrew Facini, Publications and Design Coordinator,
Belfer Center

Acknowledgments

The D3P team would like to especially thank Heather Adkins of **Google**, Yasmin Green of **Jigsaw**, the **Hewlett Foundation**, the **Democracy Fund**, and the **Belfer Family**; without whom this Playbook would not have been possible. Additionally, we would like to thank the following organizations and offices for sharing their time with us through conversations, simulation participation, or field visits. Your perspectives were critical in shaping our approach to this document.

Department of Homeland Security (DHS)

National Association of State Election Directors (NASED)

National Association of Secretaries of State (NASS)

National Governors Association (NGA)

National Guard Bureau (NGB)

Election Officials from the Following States and Jurisdictions:

Atlantic County, New Jersey

Nevada County, California

Orange County, California

Santa Clara County, California

State of Colorado

Arapahoe County, Colorado

City and County of Denver, Colorado

State of Connecticut

Escambia County, Florida

Cook County, Illinois

State of Louisiana

State of Maryland

Caroline County, Maryland

Commonwealth of Massachusetts

State of Minnesota

State of Nevada

Clark County, Nevada

State of New Jersey

Mercer County, New Jersey

State of North Carolina

State of Ohio

State of Oregon

Multnomah County, Oregon

Commonwealth of Pennsylvania

State of Rhode Island

State of Tennessee

State of Vermont

Commonwealth of Virginia

State of West Virginia

Harrison County, West Virginia

State of Washington

State of Wisconsin

The Playbook Approach

Election officials are democracy's frontline defenders. Our election system faces an array of threats designed to undermine vote integrity and public trust in the election process. It is crucial that everyone involved in the election process—from top-level leaders, like Secretaries of State and Election Administrators, to day-to-day operators, like clerks and election site workers—understand their role in protecting the process and the threats that it faces. To this end, this Playbook has two goals: (1) to make the most likely and most serious cybersecurity and information operation threats understandable to everyone involved in the election process; and (2) to offer state and local election officials basic risk-mitigation strategies to counter these threats.

Our recommendations represent a baseline. It would be impossible for us to cover every vulnerability, as new malicious actors and attack vectors constantly emerge. For this reason, we have focused on the most likely and most serious cybersecurity and information operation risks that elections face. This is not intended to be a comprehensive technical reference for IT professionals, but implementation of some strategies will require their involvement. We also did not address every issue or policy challenge that impedes cybersecurity readiness. Instead, we focused on the vulnerabilities and threats that align to create risk to our election process.

Finally, we understand that election officials already face many challenges in delivering accessible, accurate and secure elections—not least of which are constraints on financial and staffing resources. This Playbook is written with those realities in mind.

We hope this guide will give election officials more confidence in deciding how to approach security strategies and a greater common understanding in working with the technical specialists needed to implement these strategies.

This Playbook consists of three parts:

Background: frames the elections operating environment.

Common Ground: provides 10 best practice principles applicable to every election jurisdiction and a list of research security insights by election system.

Technical Recommendations: offers basic risk-mitigation recommendations specific to five components of the election system: voter registration databases, vote casting, vote tallying, election night reporting, and internal and public communications.

Our appendices offer more specific recommendations on two complex topics: vendor selection and maintenance, and election auditing. Additionally, the D3P Team has put together two additional resources to help navigate the challenges of maintaining and preserving public trust: "The Election Cyber Incident Communications Coordination Guide" and "The Election Cyber Incident Communications Plan Template for State and Local Election Officials."

Introduction

Running elections is complicated. It requires year-round preparation and coordination. Election officials have a lot to manage to ensure that the process remains free, fair, and accessible. Historically, efforts to protect the election system have focused on physical security, but today's digital world requires that we also focus on cybersecurity and information operations to defend against malicious actors of varying motives and means.

Cyber Attack: an attack targeting a network for the purpose of disrupting, disabling, destroying, or maliciously controlling it; or an attempt to destroy the integrity of data or steal controlled information. Common attacks include: spear phishing (to gain unauthorized access to existing accounts), denial of service (DoS), and device takeover.

Information Operations: the dissemination of information, true or false, to manipulate public opinion and/or influence behavior. Digital technologies like social media have made it possible for nation-states to organize information operations at an unprecedented scale. Because the tools needed for information operations are incredibly cheap and widely accessible (all you need is access to the Internet), adversaries use information operations to gain an asymmetric advantage over the U.S. and compete for influence in the world. Common information operation tactics include: spreading fake or misleading information online, leaking stolen information online, and using social media to amplify opposing views and stir political conflict.

Cyber attack and information operations tactics are often used in coordination. For example, a malicious actor might hack an election official's email account, alter emails, and then use those stolen, altered emails to spread misinformation online. Alternatively, social media login credentials might be stolen, and an official account then used to create confusion.

Background

What's at Stake

A core tenet of democracy is that the government reflects the will of the people. Elections are the quintessential expression of this principle and citizens won't trust their government unless they trust the election process and the integrity of its outcome.

Perception is reality. An adversary can manipulate the outcome of an election through actual cyber operations, but they can get the same result (i.e., erode trust in the process) by using information operations to make the public *believe* that the election was manipulated, even if it wasn't in reality.

The U.S. intelligence community reported that cyber and information operations took place in the 2016 presidential election. While it didn't affect the outcome of the election, it did reveal significant vulnerabilities in our elections process. The 2016 case was not the first time malicious actors have meddled with U.S. elections, and it will not be the last. In January 2018, the Director of the Central Intelligence Agency, Mike Pompeo, stated he has "every expectation" Russia will continue meddling in U.S. elections, including the upcoming November 2018 midterm elections. While these foreign operations are traditionally a matter for the intelligence community and federal law enforcement, responsibility to secure elections ultimately falls on local and state officials.

Cybersecurity Threats to Elections

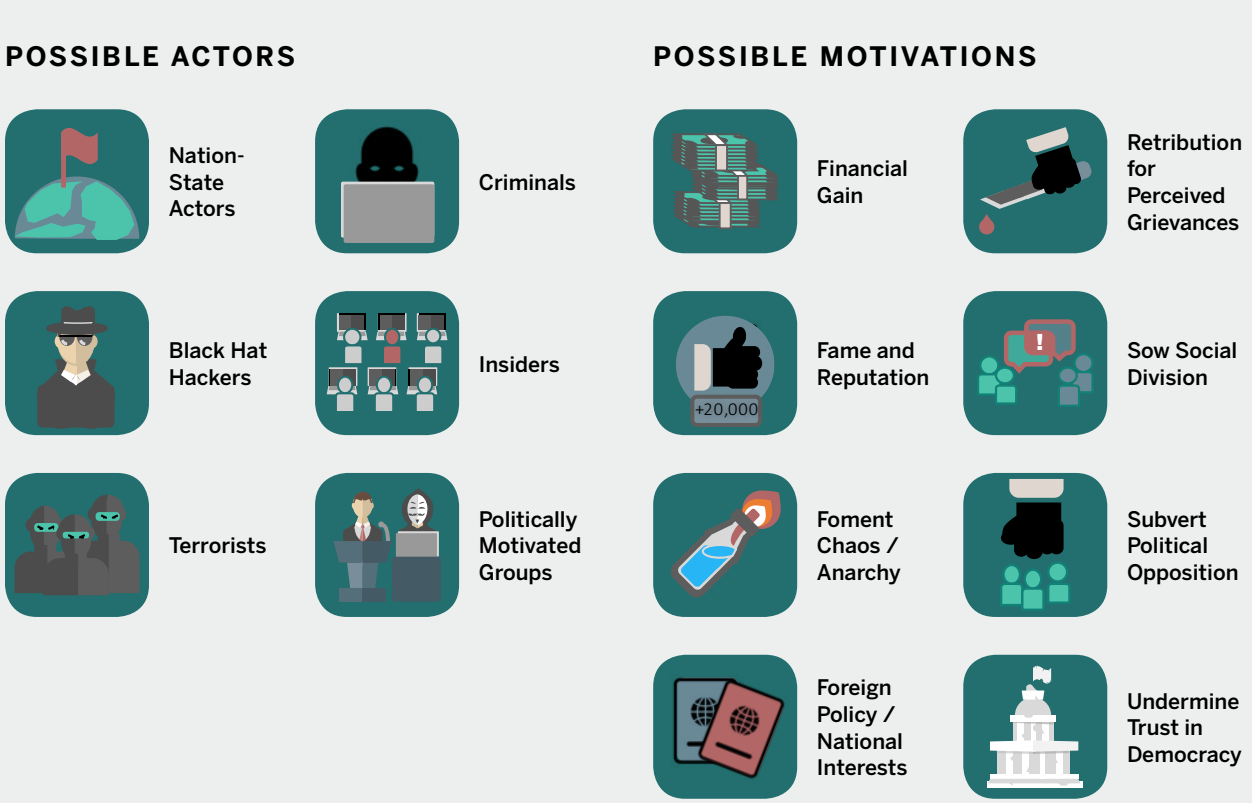
U.S. elections are decentralized. The federal government provides national-level guidance, but state and local governments administer elections. In almost every state, local officials at the county or municipal level have direct responsibility for the conduct of elections in jurisdictions ranging in size from a few dozen to nearly eight million eligible voters.

The distributed and decentralized nature of elections is both good and bad for cybersecurity. Fortunately, decentralization makes it hard, though not impossible, for a single cyber operation to compromise multiple jurisdictions. However, disparities in cybersecurity resources and

experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. Our nationwide security survey of states and territories reinforced this, with the most frequent concern noted by election officials being insufficient resources to secure the process, especially in smaller counties.

The "Who" Behind Cyber Attacks & Information Operations Targeting Elections

A range of adversaries have both the capability and intent to inflict harm on the democratic process using cyber and information operations tools. They can do this from an ocean away or right down the street. The Russian intelligence services partially achieved President Putin's goal of undermining trust in American democracy by using a combination of cyber attacks and information operations to influence narratives of the 2016 presidential election. This partial success, and the U.S. government's failure to respond sufficiently to the Russians, likely means that future elections will face attack from a broader set of actors. Nation-states pose the most well-resourced and persistent threat. Lone "black hat" hackers and cybercriminals, who may be motivated by personal gain, notoriety, or the simple desire to see if they can succeed, are also a salient threat.



See the table on page 10 for an overview of known hostile actors.

KNOWN HOSTILE ACTORS THAT COULD TARGET U.S. ELECTIONS

Russia: The Department of Homeland Security, the U.S. intelligence community, CrowdStrike, and other private sector firms implicated Russian intelligence groups "Fancy Bear" and "Cozy Bear" in the 2016 U.S. presidential campaign hacks. Russian meddlers also probed information systems related to voter registration in 21 states, gaining access to at least two systems. Media sources also reported Russian hackers allegedly penetrated a U.S. election software vendor, hoping to gain information for a subsequent spear-phishing campaign against state and county election officials. In the run-up to (as well as since) the 2016 election, Russian-affiliated groups have conducted information operations using social media sites, exploiting existing fissures in American society. Similar coordinated efforts combining cyber attacks and information operations attempted to influence the 2014 Ukrainian and 2017 French elections.

China: In the 2008 and 2012 U.S. presidential elections, Chinese hackers are believed to have penetrated Democratic and Republican presidential campaigns. These breaches appear to have been focused on intelligence gathering as there is no evidence hackers released stolen materials, or attempted to interfere with state election systems.

Iran: In 2016, the U.S. Justice Department identified Iran as the culprit in a 2013 cyber attack against a small piece of U.S. physical infrastructure, as well as a series of denial of service attacks on major U.S. financial institutions. Iran demonstrated strong cyber operational capabilities during its penetration of U.S. Navy unclassified networks in 2013. If geopolitical tensions with Iran rise, Iran's cyberspace capabilities could pose a future threat to U.S. elections.

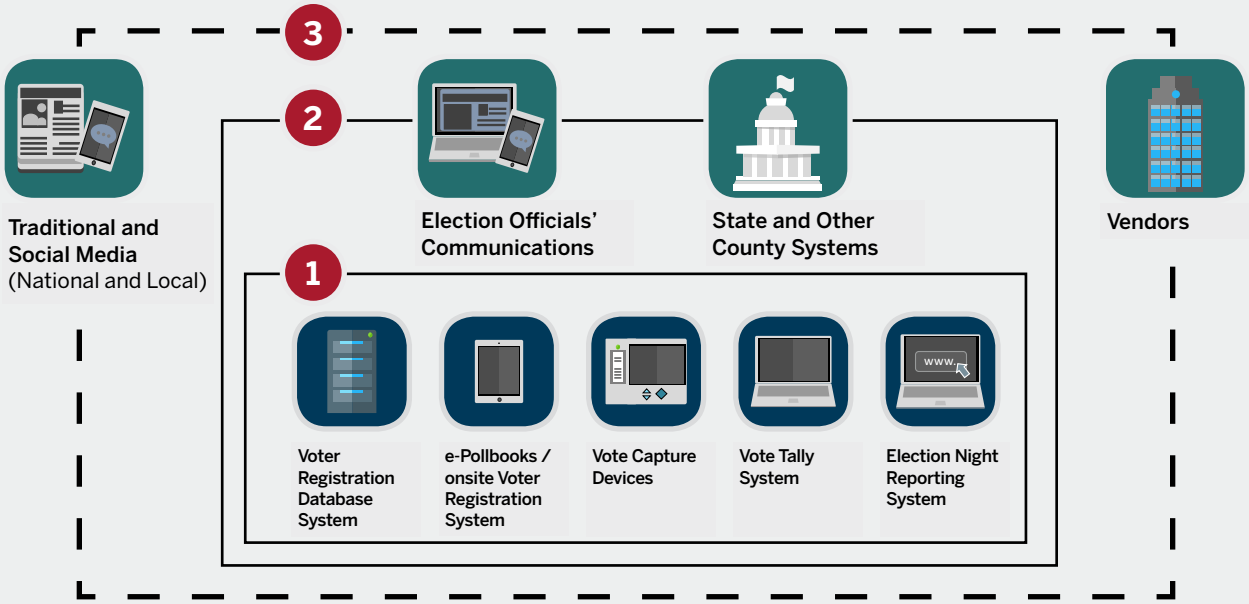
North Korea: While there is no evidence to date of North Korean election-related hacking, the regime has targeted other industries. North Korean hackers infamously retaliated against Sony Pictures Entertainment for producing the film "The Interview" by stealing and releasing company emails and wiping out large parts of Sony's information systems. The U.S. government has attributed the "WannaCry" campaign, which damaged computers across the world, including the U.K. National Health Service, to North Korea. Additionally, government-linked hackers have conducted a series of cyber attacks on financial institutions, central banks, and the global SWIFT financial transaction system, with the aim of raising money for the regime. Heightening tensions between North Korea and the U.S. could provide North Korea with incentive to undermine American democracy, and prompt future attacks.

The "How" Behind Cyber Attacks and Information Operations Targeting Elections

From a cyber perspective, every part of the election process that involves some type of electronic device or software is vulnerable to exploitation or disruption. When discussing election cybersecurity, the focus is often on voting machines. However, voting machines are only one part of a complex, interconnected system. Securing elections requires securing the entire process, because any element of the system could be the weak point that a malicious actor exploits.

We have broken the election system and its components into three levels of operation relating to cybersecurity risk. Officials in all jurisdictions, regardless of size, must secure the process at each level. The first level ❶ includes the core systems that make elections run: voter registration databases (VRDBs), electronic poll books, vote capture devices, vote tally systems, and election night reporting (ENR) systems. The second level ❷ includes two intermediary government functions that connect to multiple election system components: other state and county-level systems, and election officials' internal communication channels. The third level ❸ involves external functions that touch the entirety of the elections process: vendors, and traditional and social media at the local and national level.

ELECTION SYSTEM OVERVIEW: POTENTIAL ATTACK VECTORS



Computers and software are present in every component of the election process, which means so are vulnerabilities. Depending on a malicious actor's motives, they could look to actually undermine the integrity of the vote, diminish public confidence in the process, or both. The potential attack vectors into an election system are both technical and human. They include those who develop and maintain the system, as well as the system itself. Ultimately, most cybersecurity breaches result from malicious actors exploiting human behavior, not technical shortcomings. This is true across all sectors and industries, and election systems will likely be no exception. Vendors of election systems or election software are also easy, valuable targets for malicious actors.

THE EXTENT OF VENDOR INVOLVEMENT IN ELECTIONS

Vendors play a critical role in supporting elections at both the state and local levels: from the computers used to access information, the servers that house information, the management of the databases that contain the information, the machines used to cast and tally votes, the websites and software used to display information and results, to the software that creates ballot designs or helps transfer information across systems. Some vendors are involved on such a broad scale that they can become a single point of failure at a national or state level. For example, over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. In the 2012 presidential election, this vendor produced over 100 million ballots in more than 4,500 election jurisdictions and 40 states. The same single point of failure can exist at the state level. For example, one state contracted with a single vendor to do all of its state maintenance and ballot definition files for the 2018 elections.

The following figure describes common cyber and information operations that target each level of the election system. It provides a basic overview of the threats that election officials face from malicious actors.

Cyber and Information Operations

Some of the most common means and methods behind cyber and information operations used by malicious actors to target elections.

CYBER OPERATIONS

Social engineering is a category of attack in which malicious actors manipulate their target into performing a given action or divulging certain information (often a login or password).

Spear-phishing is a social engineering attack in which malicious actors send an email attachment or link that is designed to infect a device or obtain sensitive information. Malicious actors often review a target's social media accounts and work environment to tailor an email to appear enticing and convincing.

Hacking refers to attacks that exploit or manipulate a target system in order to disrupt or gain unauthorized access.

SQL injection is a way for attackers to read and/or alter the contents of a user's database by manipulating forms that are publicly available or exposed. Properly validating any incoming information from users can help prevent this method of attack.

Port scans are similar to checking whether doors are locked and walking through those that are open. Attackers often use it to profile potential targets and conduct surveillance on the systems they are running. A skilled attacker can use this method to gain access to unprotected servers or networks.

Man in the middle (MITM) attacks occur when attackers insert themselves between two or more parties and gain access to any information in transit between those parties.

Distributed Denial of service (DDoS) attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access. Attackers disrupt service by using multiple computers and Internet connections to flood a target with excessive traffic, causing the service to crash.

Insider threat is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes.

INFORMATION OPERATIONS

Information Operations (IO) include propaganda, disinformation, and other tools used to manipulate public perception. Digital technologies have enabled adversaries to conduct IO at an unprecedented scale and to an unprecedented effect. In the context of elections, adversaries might use IO to undermine trust in an election result, exacerbate political divisions, or sow confusion and dissent.

Leaking stolen information: Attackers penetrate networks to obtain and leak sensitive information. Leaking information about budgets, election system vulnerabilities, or sensitive processes can reduce public trust.

Spreading false or misleading information: Attackers may hijack official accounts, or use social media or paid ads to distribute false information (e.g., polling times/places, election results), discredit a candidate, election officials, or voting system integrity.

Amplifying divisive content: Malicious actors often use existing social or political tensions to stoke divisions, distract, and disrupt a target to divert their resources.

Interrupting service to public-facing online resources: Attackers may use this tactic to accomplish a broader strategic objective. A DoS attack can serve to undermine trust in electoral systems or government services.

Common Ground

10 Best Practices that Apply to all Election Jurisdictions

Despite variations in election systems across states and localities, our 10 best practices can make any jurisdiction more secure. The list below provides overarching, high-level concepts. In the Technical Recommendations section, we operationalize these best practices into risk-mitigating recommendations addressing five components of the election system: voter registration databases, vote casting, vote tallying systems, election night reporting, and internal and public communications.

1. **Create a proactive security culture**. Risk mitigation starts with strong leaders who encourage staff to take all aspects of election security seriously. Most technical compromises start with human error—a strong security culture can help prevent that. A strong security culture also makes a big difference as to whether a malicious actor: (1) chooses to target an organization, (2) is able to successfully do so, or (3) is able to create public perception that the organization has been compromised. Any state could experience a cybersecurity threat to their elections process—it is the job of leaders to make sure they are prepared.

   Lead by example. Senior leadership, especially Secretaries of State, Election Administrators, and other heads of municipal jurisdictions, need to set an example for the rest of the organization. Issue guidance about the necessity of applying cybersecurity standards (such as those recommended in this Playbook), stressing the importance of cybersecurity for staff by personally introducing orientations and trainings, and following up with operations personnel on a regular basis about the implementation of improved cybersecurity protections. Leaders also need to ensure that those charged with implementing a cybersecurity program have the authority to enforce policies and procedures. Without enforcement, these are only words on paper.

   Develop a detailed cyber incident response plan. As with contingency plans for physical threats, teams should understand critical election system vulnerability points and create a detailed response plan (both internal processes and communications) for any system compromise. Leadership should also mandate frequent testing of critical systems to ensure both their resilience and officials' comfort with crisis management. Officials should extensively document any real or simulated incidents and review these periodically for training purposes.

   Use external resources to assist in improving cyber defense capabilities and building expertise. Department of Homeland Security and private sector technology companies are

available to provide support for prevention and detection. Recognizing Constitutional and other legal restraints, National Guard cyber units, operating under state authorities, can also be a resource to help identify network vulnerabilities. These units are often made up of highly trained professionals involved in private sector cybersecurity.

Be diligent in selecting who is involved in election administration. Election systems qualify as national critical infrastructure, which raises the security expectations for those involved. Conduct background checks on all personnel involved in accessing sensitive information and privileged systems. Require vendors to do the same.

2. **Treat elections as an interconnected system**. Adversaries can target not only individual parts of the elections process but also the connections between them. Attackers look for seams: they seek the weakest point and move from there to their intended target. External systems (e.g., Department of Motor Vehicles databases and vendors) with election system access must be included in the system landscape because they can be penetrated to gain access. The compromise of one part of the election system or an external source can potentially corrupt seemingly unrelated parts of the system. This is true even if the system is not technically connected to the Internet—hacks can be executed using thumb drives and other external storage devices.

Safeguard computers and digital devices that touch the process, regardless of whether they are owned by a vendor, the state or local government, or are the personal device of an official or volunteer.

Centralize and streamline device security management by incorporating election offices into existing technology security plans.

3. **Have a paper vote record.** To protect against cyber attacks or technology failures jeopardizing an election, it is essential to have a voter-verified auditable paper record to allow votes to be cross-checked against electronic results. Without a paper vote record, accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software, and data; every aspect from the ballot displayed to the voter to the recording and reporting of votes, is under control of hardware and software. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or reload new and maliciously behaving) software running on a machine that does not produce a paper record, not only has the potential to alter the vote tally but can also make it impossible to conduct a meaningful audit or recount (or even to detect that an attack has occurred) after the fact.

Create an auditable paper record for every vote cast that is verified by the voter to ensure if the electronic vote count is maliciously altered, a true record still exists on paper. Make sure that this verifiable paper record has a rigorous chain of custody associated with it.

4. **Use audits to show transparency and maintain trust in the elections process.** Audits are a mechanism to detect intrusions or manipulations on electronic systems that may go unnoticed and reassure the public that the elections process works. This is an important part of the public engagement strategy that builds confidence and demonstrates transparency. *When combined with #3, having an auditable paper vote record, this substantially reduces the risk of a malicious actor delegitimizing an election.*

> **Embed auditing** at points in the process where data integrity and accuracy are critical; for example, with voter registration records.

> **Make post-election audits standard practice**, using paper records to confirm electronic results.

5. **Implement strong passwords and two-factor authentication.** Malicious actors frequently use stolen user credentials (e.g., username and password) to infiltrate networks. Although strong passwords are important, *two-factor authentication is one of the best defenses* against account compromise. Two-factor authentication typically requires a user to present something they *know* (a username/password) and something they *have* (such as another associated device or token) in order to access a digital account. Only by having *both of* these things will the user confirm their identity and be able to gain access to the system.

> **Require strong passwords** not only for official accounts but also for key officials' private email and social media accounts. For your passwords, create `SomethingReallyLongLikeThisString`, not something really short like `Th1$`. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with lots of `$ymB01$`.

6. **Control and actively manage access.** Everyone with access to the computer network can become a target and often only one target needs to be compromised for an attack to succeed. The more people who can use a system, and the broader their access rights, the greater the opportunities for malicious actors to steal credentials and exploit them.

> **Limit the number of people with access to the system** to those who need it to complete their jobs (the "who").

> **Restrict what each user is authorized to do** using the principle of "least privilege," meaning give users the minimum level of access that they require to perform their jobs (the "what"). For example, not every official from County A needs the ability to view or modify voter registration records in County B.

> **Quickly remove those who no longer need access**, regardless of their privilege level. Make this a part of standard offboarding procedures for staff.

7. **Prioritize and isolate sensitive data and systems.** Risk is where threats and vulnerabilities meet. To reduce risk, officials need to think about what vulnerabilities will cause the most damage, given the threat environment. Officials consider two things when making a risk assessment: (1) what data is most sensitive and (2) what disruption could be most damaging to voters' trust in the election. They should then prioritize mitigating the vulnerabilities that could lead to this damage by isolating and protecting these systems the most. Every part of the system is important, but a good security strategy will determine which systems are most sensitive and prioritize efforts there, since these extra protections create operational hurdles and increase costs.

> **Configure devices with sensitive data** to only be used for their specific purpose in the elections process (e.g., the software on a vote tallying computer is only what is necessary to run the election management system; or it operates on an isolated network so all wifi/bluetooth is disabled).

> **Restrict the use of removable media devices** (e.g., USB/thumb drives, compact discs) with these systems. A "one way, one use" policy is best.

8. **Monitor, log, and back up data.** Monitoring, logging, and backing up data enables attack detection and system or data recovery after an incident. When it comes to monitoring, a combination of human and technical means is best. Local officials highly knowledgeable about their jurisdictions can identify many irregularities. However, this alone may leave gaps in detecting attacks. Automated forms of data monitoring, especially at the state level to detect cross-county patterns, are critical for detecting anomalies and highlighting when manipulation or intrusion occurs.

> **Log any changes to the voter registration database**, and monitor the database with both a human check and anomaly detection software.

> **The adage is that "your data is only as good as your last backup."** This means that (1) backups should be regularly performed, either through automation or as part of a scheduled manual process, (2) backups should be read-only once created to prevent data corruption, and (3) backups should be regularly tested by performing a complete restore from backed-up data. Database technology vendors provide guidance and best practices specific to their technology and database architecture for validating and testing restoration of backups; consult these recommendations when developing your plan. In addition to those recommendations, ensure backups are stored in a different physical location than the master database and are physically secured.

9. **Require vendors to make security a priority.** In many states, vendors design and maintain hardware and software that affect voter registration, vote capture and tallying, electronic pollbooks, election night reporting, and public communication. In our nationwide security survey, 97% of states and territories used a vendor in some capacity. Some vendors service multiple states— meaning an attack on one vendor could affect

many elections. Conversely, smaller vendors may not dedicate the necessary resources to cybersecurity, making them unable to defend against sophisticated attacks. (*For more details, see* **Appendix 1: Vendor Management***)*

Include explicit security stipulations in requests for proposals, acquisition, and maintenance contracts to ensure that vendors follow appropriate security standards, and guarantee state and local governments' ability to test systems and software.

Remember that skepticism is healthy. Verify security claims of vendors with independent analysis or reports from trained professionals.

Require vendors to provide notification of any system breach immediately after they become aware of it.

10. Build public trust and prepare for information operations.

Communication is the cornerstone of public trust. Transparency and open communication will counter information operations that seek to cast doubt over the integrity of the election system. For additional information on communication strategies and planning see the D3P "Election Cyber Incident Communications Coordination Guide" and "Election Incident Communications Plan Template".

Communicate repeatedly with the public to reinforce the message that integrity is a top priority.

Before elections are held, start informing the public about cybersecurity threats, the steps taken to counter them (withhold specific details that could aid an attacker), and your readiness to respond in the event of an attack.

Establish processes and communications materials to respond confidently and competently in the event of an attack.

Build relationships with reporters, influencers, and key stakeholders to establish trust and have good communications channels before an incident occurs. It is especially important to do this with candidates and party officials.

Routinely monitor social media, email accounts, and official websites, and establish points of contact with social media firms (e.g., Facebook, Twitter) to enable quick recovery of hacked accounts.

Security Insights by Election System

During our field research we learned a lot of great insights from election officials who are making cybersecurity a reality. This list reflects many of those ground-level insights, classified by the key components of the election system. For detailed technical specifications, refer to the Technical Recommendations section.

VRDB

- Patch and update all computers and servers that connect to the database.
- Ensure the database server is not accessible over the public Internet. Restrict which external systems can write directly to the database.
- Establish a baseline for normal data activity (new entries and edits to existing entries). Monitor activity against this baseline and investigate anomalies. Add human review for data changes—at a minimum, review weekly change summaries; ideally have an official review automated updates.
- Limit access to only those who need it. For those with access, restrict access to only their area of responsibility (e.g., a county official can only edit files for his/her county but may have read access to others). Regularly adjust access and permissions as personnel change.
- Require two-factor authentication for anyone to log into the database—no exceptions.
- Make frequent backups of the VRDB. Conduct routine recovery drills to ensure they work.

For Online Voter Registration

- Do NOT allow web servers to connect directly to the VRDB.
- Have mechanisms in place to mitigate DDoS attacks on the voter registration website.

For e-Pollbooks

- Restrict device functionality to only what is required and confirm, through pen-testing, that all unnecessary features are disabled (e.g., wifi, bluetooth). Disable functionality in hardware when possible.
- Make them single-purpose devices; software on them should only be what is necessary.
- Understand how voter information is loaded onto the e-Pollbooks; cryptographically confirm the e-Pollbook file on the device matches the original file.
- Physically disable or otherwise seal exposed ports if possible.

Vote Casting Devices

- Every machine should have an individual voter-verified paper trail.
- Do election audits. Make them a regular part of the elections process.
- Restrict device functionality to only what is required and confirm, through pen-testing, that all unnecessary features are disabled (e.g., wifi, bluetooth). Disable functionality in hardware when possible.
- Do not connect machines to any network for longer than necessary (i.e., if wifi is used to update, ensure it is enabled only for the required time window).

If vote tallies are transmitted directly from the machine, ensure the data transmission is encrypted.

Treat all removable media as a potential delivery mechanism for malware. Institute a "one-way, one-use policy:" only use physical media once, from one system to a second system, then securely dispose of it.

Ballot definition files could be corrupted—secure the creation, transfer, and upload process.

Vote Tallying Systems

Vote tallying systems should be single-purpose systems, with only software installed required for running the vote tallying system—nothing else, and isolated with no network or Internet connectivity.

Electronic vote tabulation data should be encrypted when transmitted between sites.

Address security vulnerabilities by patching and updating vote tallying system devices.

Use two different forms of communication to report and confirm vote tally reports (e.g., electronic file submission, then phone call).

Treat all removable media as a potential delivery mechanism for malware. Institute a "one-way, one-use policy." Only use physical media once, from one system to a second system, then securely dispose of it.

Election Night Reporting

Ensure websites are up to date and create a plan for DDoS mitigation.

Limit access/edit privileges for users, similar to VRDB access.

Prepare a contingency communications plan for disseminating results.

Verify that results shown to the public on the official ENR website match reported results.

Monitor the ENR system for anomalies in traffic or access during election night.

Conduct searches/media reviews during election night to check for false sites and social media accounts.

Internal and public-facing communications

Email: Use two-factor authentication for email accounts.

Public-facing websites beyond ENR (e.g., to communicate election day logistics): Keep sites up to date to decrease potential for manipulation; have an action plan for potential DoS; know how to recover hijacked accounts.

Official social media accounts: Use two-factor authentication. Limit access. Understand third-party apps can be a vulnerability if they are compromised. Identify points of contact and establish relationships with key social media firms for responding to issues when they arise. Know how to recover hijacked accounts.

Private social media accounts: Private accounts of key officials need to be secured as they are also likely targets.

Vendors

Require vendor security measures. Vendors can connect to every part of this system. Their internal security matters—vendor access points could be the weak link that gets exploited and corrupts other parts of the process.

Ensure security requirements and considerations are included in vendor contracting and enforced.

Technical Recommendations

Securing State Election Systems

There is no such thing as perfect security; however, there are preventative measures that make the process much more secure. In the Common Ground section, we provided best practices that apply across all election jurisdictions and some system-specific insights. In this section, we elaborate on these concepts with specific technical recommendations as they relate to five components of the election system: voter registration databases, vote casting, vote tallying systems, election night reporting, and internal and public communications. As we highlighted in Common Ground, system defense is a critical first step in securing the elections process. For this reason, the majority of our recommendations fall into the category of "Protect." Because election systems are decentralized and varied in nature, not all recommendations apply to every state or locality.

As we said in the introduction, our recommendations represent a baseline. It would be impossible for us to cover every vulnerability, as new malicious actors and attack vectors constantly emerge. For this reason, we have focused on the most likely and most serious cybersecurity and information operation risks that elections face. This is not intended to be a comprehensive technical reference for IT professionals. But we do want to emphasize IT professionals are critical to establishing and maintaining a secure election system and their expertise will be needed for many of our recommendations. Threats are constantly evolving and IT professionals will help you get beyond what this Playbook provides and keep you abreast of the latest threats and defenses.

Voter Registration Databases and e-Pollbooks

Voter registration databases (VRDBs) store information on registered voters in a given state. The Help America Vote Act requires that all states implement a "single, uniform, official, centralized, interactive, computerized voter registration list," unless the state has no voter registration requirement. Throughout this document, we refer to this centralized, computerized list as the VRDB.

Different states follow different processes for managing and updating their VRDB—in some states, all new entries, deletions, and edits are implemented as processes at the state level, whereas in other states this happens at the county level (with changes pushed up to the state-held "master"). In many states, ***third-party systems***, such as Health and Human Services and the Department of Motor Vehicles, provide data to the VRDB in an effort to keep voter records up to date. Some states offer ***online registration***, allowing voters to register and edit their record via a public-facing online portal connected to the VRDB. Some states offer ***same-day registration***, while others require voters to register before election day.

Closely linked to VRDBs are the pollbooks used on election day. States may choose to only use paper pollbooks, or may use ***electronic pollbooks (e-Pollbooks)*** to process voters on election day. e-Pollbooks are electronic versions of voter rolls used by polling site officials to verify legal voter registration and related details on election day. These are usually tablets or laptops and can be networked into a central voter registration system (allowing them to check and update voter records in real time, for example to allow for same-day voter registration), or they can be standalone at the precinct (containing a separate, offline copy of the electors list). Regardless of whether a state/county uses paper or e-Pollbooks, their creation requires an export of files from the VRDB for either printing or translation into an e-Pollbook compatible file.

Across both VRDBs and e-Pollbooks, states may choose to develop and maintain the software in-house, or may outsource this work to an external ***vendor***.

Core VRDB issues

KEY THREATS:

Unauthorized access to the VRDB from Internet exposure: Leaving the VRDB exposed to the Internet makes it vulnerable to attacks. Once it is connected to the database, an attacker can add, edit, or delete voters, allowing for false votes to be cast on election day or forcing voters to cast provisional ballots. Even if this does not affect actual vote outcomes, the perception of vote manipulation or voter suppression can significantly undermine the credibility of an election.

Maintenance: An insufficient or poorly timed maintenance and patching regime leaves security vulnerabilities open and can expose the VRDB to attacks.

Account compromise: Attackers might compromise the accounts of election officials with access to the VRDB; without proper controls in place this could allow the attacker to add, edit, or delete voter entries. In the absence of proper logging and monitoring, these changes may go unnoticed until election day and affect the ability of voters to cast ballots.

Third-party system compromise: Third-party systems (e.g., DMV, HHS) linking into the VRDB can be compromised, or the transmission of these entries to the database could be compromised along the way. If these systems are allowed to feed directly into the VRDB, or if the review and approval process at the state and county level is insufficient, there is a risk that the compromise could allow malicious actors to manipulate voter status.

Recommended actions:

Identify

Map how other systems connect to the VRDB. They will commonly be connected to sync or add voter information (e.g., from DMV records).

Know where the VRDB is hosted and what defenses exist on the servers and the underlying network infrastructure.

Know what accounts have access and what level of access each account has (e.g., can a county official change records from other counties?). Use a test account to verify that restrictions are operating as intended.

Determine which of the servers can be accessed over the Internet. Close connections to any that do not require access.

Protect

Require strong passwords and implement two-factor authentication. This should apply to everyone who can edit the VRDB. Account security is crucial for all VRDB users and especially those with elevated or administrative privileges.

Conduct penetration tests, source code audits, and encourage vulnerability discovery efforts. Regardless of whether your VRDB software is built in-house or by vendors, third-party auditing and penetration testing should be performed to provide awareness of security vulnerabilities. Develop and maintain a continuous program that tests your organization's susceptibility to spear phishing and other social engineering attempts. It is important to do this regularly, both to spot new vulnerabilities that might arise, and to prevent staff from becoming complacent.

Apply software updates and patches. Applying software updates and patches on all devices connecting to the VRDB is essential to preventing malicious actors from gaining access. Check for patch signatures to ensure they are authentic. Using endpoint management software and vulnerability software on official computers can help automate the patching process to ensure systems stay up to date.

> To prevent interference with election day operations, **establish cut-off days for applying and testing patches** to ensure optimal functionality during election periods. Only critical updates should be done after the cut-off window and all patches should be tested for functionality as well as security.

> **Create automated scans** to look for vulnerabilities on the VRDB portal.

Ensure that your underlying database server is not accessible over the Internet.

Restrict external systems' access to the VRDB. Data from other systems (e.g., the DMV) should go through validation (either manual or automated) rather than allowing those systems to directly write to the database. This prevents the database from being directly edited if an external system is compromised.

Log changes. As a rule, changes to the VRDB should be recorded securely and be reviewed, preferably both by a human and an automated system. Establish a baseline for normal data activity (e.g., new entries, edits to existing entries, change in voter status) so that atypical behavior can trigger an alert.

Limit account access to the VRDB. Restrict access to the database to those who need it and diligently maintain and review this access list. For example, state or local offices responsible for updating voter registration information require access. However, the software developers who designed the system do not. Account management includes revoking the access of old employee accounts immediately after they depart or change roles. Vendors responsible for the software will need access, but should not retain that access any longer than necessary.

Implementing these limitations requires an individual to be responsible for constantly managing accounts, ensuring existing accounts belong only to those who need them, and that system permission changes were approved.

Permissions Management for VRDB accounts. Everyone who has an account should be given specific permissions that dictate what they can and cannot do. More people with more access means an increase in potential avenues of attack on the VRDB, so limit the degree of access for each account to only what is necessary for that employee to do their job.

The most common levels of permission variation are "read," "write," and "admin" access. Someone with "read" access can only read the data, but not alter it; someone with "write" access can change data; and someone with "admin" access can alter permissions for other users.

Even within those levels of permissions the scope of access should be tailored. For example, a county administrator may need access to their own county's information, but should not be able to access information from another county.

Consider implementing permission restrictions that limit the number of changes one user can make during a certain time window to stay in line with normal activity patterns—this helps guard against both insider threats and account compromise.

Require users to access the VRDB portal using a VPN. This ensures that even if an account is compromised, the attacker is unable to use it without VPN credentials.

Whitelisting can also be used to limit either what devices a user can connect from or which locations. Paired with a device inventory database, requiring device certificates will allow you to restrict access to managed devices that are verified as secure. Another option is IP whitelisting, which can restrict access to users at specific location. This would require coordination with remote offices' IT departments to identify what addresses should be whitelisted. Using IP whitelists would force an attacker to compromise a machine at one of the locations before they were able to begin an attack against the VRDB.

Establish policy that does not allow connections to the VRDB from public, unauthorized, or unknown devices.

Detect

Monitor activity against a baseline and investigate anomalies. This allows you to notice unusual trends that deviate from the norm. At a minimum, this should be a technical (automated) check which occurs at both the state and county level. Automated monitoring of anomalies at the state level is critical to detect broad changes across the state that may not be noticeable when monitoring only at the individual county level.

Incorporate a human review into data change monitoring to augment technical monitoring. Experienced election officials providing human monitoring at the local level may reveal subtle manipulations. Election officials should trust their instincts—they are more

familiar with this data than anyone else. Empower these officials to flag suspicious behavior or anomalies and investigate them. While human review of every record change is not realistic for all localities, weekly change summaries should be required at a minimum.

Monitor permission changes: Make sure that when changes are made, they are reviewable by those with similar access levels. Create the framework for conducting regular reviews of those changes. This process will allow unusual activity to be detected sooner.

Mail confirmation of changes in registration to voters (ideally both to their old and new address).

Respond

If the incident involved an attacker gaining access to VRDB, perform a thorough review of the system's accounts and access controls to ensure that any backdoor the attacker might have left open is purged.

If a physical machine was compromised, disconnect the machine from the network and seek professional forensic assistance. Discard the machine afterwards: reformatting the machine is not always sufficient to remove exploits. If the machine was connected to any other machines, systems, or components, review those as well.

Recover

Execute the recovery plan during an incident or after one occurs. Include the following categories in your plan: Recovery planning, improvements, and communications.

Public communications around a voter registration-related incident is a CRITICALLY IMPORTANT issue when it comes to public trust and elections transparency. It must be deliberately executed with tremendous care. See D3P's *Elections Cyber Incident Communications Plan Template*.

Practice restoring from VRDB backups. If there is a second live VRDB system, be sure to practice using the secondary system.

Lessons learned should be shared and incorporated into the existing recovery plan. Where possible, update your system to prevent a similar failure or exploit from occuring again in the future.

Vendor Considerations

The most common forms of vendor support for voter registration databases are:

- Vendors building and maintaining the VRDB
- Vendor building and state or county maintaining of the VRDB (to include modifications to initial vendor build)
- Vendor and state jointly building and maintaining
- Third party vendor used to assist with maintenance

The General Vendor Recommendations 1-8 at the bottom of the Technical Recommendations section provide best practices for working with vendors and mitigating potential cyber vulnerabilities. The type of vendor involvement and timeframe (set time period involvement versus continuous) will impact how they apply for each state/county. Additional contract specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Online Voter Registration

States that offer online registration are exposed to the following additional threats:

KEY THREATS:

Website spoofing: Attackers could pose as the official website to either give voters the illusion that their information is updated or in an attempt to capture that information.

Distributed Denial of Service: Attackers can conduct DDoS attacks on the public-facing voter registration website, preventing voters from registering and potentially discouraging them from participation.

External connectivity: An unsecured website presents another vector for a malicious actor to penetrate the VRDB. If it is not properly secured, an attacker may be able to use it to change any vote record.

Large-scale data alteration: An attacker could use information leaked on the Internet to impersonate many different voters and attempt to update their registration details.

Recommended actions:

Identify

- Know who the domain name registrar and web hosting provider are and how to contact them.
- Determine who is responsible for keeping the website software up-to-date.
- Know who has the ability to edit the website.

Protect

- Do NOT allow web servers to connect directly to the VRDB. This restriction significantly reduces the possibility of a website vulnerability leading to a compromise of voter records.
- Require a CAPTCHA to change a voter's registration. This is a short task, ranging from clicking a checkbox to typing the characters shown in an image, which verifies that an online form is being submitted by a human and not a machine. It increases the difficulty of a computer program changing hundreds or thousands of voter registrations at once.
- Protect the online voter registration website against DDoS attacks.
- See the **Website** section for additional details on securing the public-facing component.

e-Pollbooks

KEY THREATS:

e-Pollbook Data Manipulation: A malicious actor is able to gain access to the device either using a wireless connection or because the physical device was not properly secured. Once on the device they are able to manipulate the voting roll—either deleting or altering existing voter registration data.

Altering of State Voter Roll via e-Pollbook: If an e-Pollbook has a live connection to the state election day voter roll, compromising one device could be used to change statewide records.

Maintenance/patching of e-Pollbooks: The difficulty in which an e-Pollbook device is compromised depends heavily on whether it is updated and patched. Failure to do so will provide malicious actors an opening into the device.

Recommended actions:

Identify

Examine all the possible functionalities of the device and identify the components you intend to use. Specifically pay attention to the wireless and networking functionality.

Know what kind of network connections your e-Pollbooks need.

Understand how voter information is loaded onto the e-Pollbooks.

Protect

E-Pollbooks should be single-purpose devices. Software on the device should be limited to what is necessary for their use.

Verify the integrity of the e-Pollbook file.

Cross-check the data on the pollbook with what is in the VRDB.

Use digital signatures and hashes to verify the integrity of data contained in voter roll files that are transferred between systems and to ensure data has not been maliciously altered or compromised. If using a method that requires data transmission over a cellular network or the public Internet, use a virtual private network (VPN) to secure those transmissions.

VERIFYING FILE INTEGRITY USING HASHES AND DIGITAL SIGNATURES

A hash is like a fingerprint for digital files—the *hash* of a file will not change unless the actual file changes. Using a hash while transferring files will allow you to confirm that the file has not been altered in transit if the hashes computed by each party are the same. If you decide to use a hash, transfer it through a different channel than you used to obtain the files and compare it to the hash you compute. By sending them separately, such as downloading the file from a website and reading out the hash over the phone, you prevent the attacker from changing the hash at the same time as the file.

A more secure option is to use a digital signature. It is a form of encryption which is equivalent to a seal on a physical document; it guarantees that the file came from a specific trusted source and that its contents have not been modified in transit.

Ensure all devices are updated and patched. Test the e-Pollbook to ensure that it is fully functional after patches have been applied.

If you do not need the e-Pollbook to be connected to a vendor, VRDB, or the Internet while voting is taking place: **turn off bluetooth and wireless capabilities on the devices.** It is better to disable these functions at the hardware level (e.g., removing the wireless card) than to change a setting whenever possible.

If you need to connect to external systems:

- **Connect over a VPN** or other encrypted channel.
- **Ensure that the entire setup is preconfigured** and that turning on devices is the only action required by election site workers (they should not need to change any settings on the devices).
- **Do not connect e-Pollbooks directly to the VRDB.** Set up a separate system (essentially a copy of the VRDB) to handle changes to voter information, which prevents the VRDB from being impacted if an e-Pollbook is compromised.
- **Restrict edit access only to juridictions that need it.** If state law requires you to vote in precinct and there is not same-day registration, an e-Pollbook in one precinct should not be able to modify the voter's record from another precinct.

Have a paper backup of the e-Pollbook.

Ensure physical security. Cover exposed ports (e.g., USB) to prevent them from being accessed by anyone intending to inject malware via a USB or other portable device. Do not use anything other than the charging cords provided with the e-Pollbook on receipt (e.g., do not use an iPhone charger or other similar charger that is not actually part of the e-Pollbook election day pack).

Detect

Monitor data changes. Counties or vendors, as applicable, should monitor voter roll files for anomalies in changes or access. Implement data controls around normal data activity that prevent large-scale changes.

Perform vulnerability scans of e-Pollbook devices to identify those that do not have the latest security updates. Apply patches to minimize vulnerabilities.

Respond

If the incident involved an attacker gaining access to a networked voter roll file shared beyond a single polling site, perform a thorough review of the system's accounts and access controls to ensure that any backdoor the attacker might have left open is purged.

If the e-Pollbook device was compromised, disconnect the machine from the network and seek out professional forensic assistance. Discard the machine afterwards: reformatting the machine is not always sufficient to remove exploits. If the machine was connected to any other machines, systems, or components, review those as well.

Recover

Have a backup paper copy of the pollbook on site and backup devices pre-programmed for deployment to sites, if necessary.

Vendor Considerations

The most common forms of vendor support for e-Pollbooks are:

- Building and/or maintaining of e-Pollbook devices and software.
  - Can overlap with vendor support for VRDBs.
  - Can involve live monitoring of e-Pollbook operations on election day.
- Building electronic voter roll files for e-Pollbooks based on VRDB info where a compromise of the vendor could result in voters being missing, or incorrectly added to, the roll.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance.**

Vote Casting Devices

Overview: Vote casting devices serve as the primary conduit for the actual ballot marking or mark recording process on election day. Most states and counties today use some variation on two types of vote casting devices:

> **Optical Scanner (OS) or Digital Image Scanner:** A machine that scans (and often digitally records an image of) marked paper ballots. Voters cast a ballot via traditional pen and paper, an electronic ballot marking device, or some alternative marking method. The marked paper ballots are then run through these scanning machines which records the appropriately marked vote for each race, and then calculates running vote totals for all ballots scanned on the machine. The machine prints a total result after polls close. The initial paper ballot ensures that a physical record exists for audit or other vote verification purposes.

> **Direct Recording Electronic (DRE):** A DRE system presents a digital ballot image to a voter, collects the voter's selections, and records those choices directly onto electronic media. DREs may be fitted with voter-verified paper audit trail (VVPAT) subsystems to create a paper artifact of the voting transaction.

In recent years, alternate voting methods, particularly vote-by-mail and early voting, are becoming increasingly popular with voters. These jurisdictions often utilize central count facilities where paper ballots are consolidated for tallying. At central count facilities larger variations of the optical scanner/digital image scanner are often used for paper ballot counting.

KEY THREATS:

Device tampering: Voting machines can be compromised via physical tampering (including using removable media) or through external connectivity (e.g., WiFi). This would allow the attacker to change the reported vote information.

Inability to detect tampering: Some DRE machines do not produce a VVPAT (because optical scanner systems scan paper ballots, they do not face this threat). Should a malicious actor compromise such a machine, votes could be lost and results thrown into question.

Recommended actions:

Identify

Examine all the possible functionalities of the device and of any of its subcomponents. Specifically pay attention to the wireless and networking functionality.

Know the certification status of all your equipment. The Election Assistance Commission's (EAC) Voluntary Voting System Guidelines (VVSG) provides federal level certification standards. Many states have their own certification process.

Protect

If you have a DRE machine that does not produce a paper trail, **you should either replace the device or purchase an add-on (VVPAT adapter) that creates a paper trail.**

Physical Security/Access Seals. Use serialized tamper-evident security seals and chain of custody logs to limit physical access to voting machines and track whenever removable media is plugged into the scanners.

Penetration test systems. Conduct, or hire a third-party firm to conduct, a source code audit and penetration test of all vote casting devices.

Restrict device functionality to what is required. Even if you have disabled a feature through a settings page (such as wifi connectivity), those features could still be exploited. You should not trust that toggling a switch in software will actually disable the functionality. If possible, the hardware should be removed.

Isolate the device from external connectivity. Do not connect the device to a network, which includes not using a cellular modem. If network connectivity cannot be avoided, make sure to keep the network connection disabled until you intend to transmit the results.

> **Create a copy of the results** (either a printout or by saving it to removable media) before you connect to the network.

If removable media is used to transfer data (e.g., ballot definition files, vote tallies):

> **Have a procurement strategy for devices.** Purchase physical media devices directly from a trusted vendor and obtain assurance that the suppliers from whom your vendors procure their memory can also be trusted. If you must use devices from an unverified source, obtain them from a location that you would not otherwise use, to make it less likely that a bad actor could plant USB devices that could infect your systems.

> **Protect device chain of custody.** Once devices are procured, ensure that they are stored securely and access is limited to the appropriate audience. When in use, maintain a physical

record of the device—including where the device has been and who has been in contact with it— to limit the opportunity for manipulation.

One-way/one-time use: Only use physical media once, from one system to a second system, then securely dispose of it. A USB device could either (1) transfer data from one air-gapped machine to another or (2) transfer data from an air-gapped machine to an outside one prior to disposal, but not both. When feasible, use write-once memory cards or write-once optical disks instead of USB devices. This ensures one-time use is self-enforced by the technology.

Scan media devices for malware. If you detect abnormalities, don't use the device and contact forensic experts for assistance.

Detect

Perform logic and accuracy testing of the programmed device.

Verify the seals and chain of custody logs via a unique identifier (e.g., seal number).

Respond and Recover

Follow the jurisdiction Incident Response and Recovery Plan for vote casting device compromise.

Vendor Considerations

Vendors are integral to vote casting devices as every device has been physically constructed, programmed, and is often maintained by various vendors. A compromise or oversight at any of these points would allow an attacker to change or erase election results.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance.**

Handling ballot definition files and other software updates

KEY THREATS

Supply chain interdiction: A malicious actor could use vendors as a pathway to plant malware to modify or compromise a ballot definition file before it reaches the hands of election officials.

Manipulation of ballot definition files: If an attacker obtains access to the original ballot definition file, this could leave machines susceptible to destructive attacks and/or could affect tallies.

Recommended actions:

Identify

Determine who is responsible for, and what machines are being used, to create the ballot definition file.

Determine how the ballot definition file is being transmitted to the vote casting device.

Protect

Treat the ballot definition file as critical information. As such, limit its exposure to compromise as much as possible. The system used to develop the file should be isolated from external network connectivity. Place a tamper-evident seal over the media containing the ballot definition file.

Conduct testing (e.g., logic and accuracy, parallel testing) on the systems that the ballot definition files have been loaded onto before deploying them for use.

Review ballot definition file source code to prevent malicious code distribution. When possible, review source code before final distribution of ballot definition files to avoid dissemination of malicious code.

Secure the creation mechanism of the ballot definition file: The ballot files should be generated on a secure single-purpose and air-gapped machine

Secure the transmission of the file:

If possible, use digital signatures on the file. Forcing the voting machines to verify the file signature before loading it will prevent attempts to change the ballot files after it has been created.

If using removable devices to transfer the files, follow all best practices, including one-way and one-time use. The section on vote casting devices above discusses more specific recommendations for removable media.

Detect

Verify the seals over media containing the ballot definition file.

Scan ballot definition files for malware. If you detect abnormalities, don't use the files and contact forensic experts for assistance.

Recover

Follow the jurisdiction Incident Response and Recovery Plan for vote casting device compromise.

Vendor Considerations

Vendors often interact with ballot files by:

- Creating the files themselves
- Transferring the ballot files to the voting machines

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance.**

Vote Tallying System

Vote tallying covers the various devices and networks used to tabulate ballots and aggregate results. Based on differences in setup across states and counties, this process can start at the polling site (for example, precinct count optical scanners that tabulate ballots onsite), or at more centralized counting facilities. In many instances vote tallying is conducted at the county level, where voting sites through a variety of methods (e.g., phone call, email, thumb drive/USB) provide counties with their respective vote tally totals. This section discusses common threats and remedies seen across many system set-ups.

KEY THREATS:

Manipulation of tabulation systems: A compromised tallying machine at a polling site or central counting facility could allow an attacker to directly manipulate tallies before they are transmitted to the county or state.

Data transmission with removable media: USB devices—and other portable physical media—are often used to transmit results from precincts or centralized counting facilities to segmented county/state networks. USB devices can be exposed to malware and compromised at the supplier level or through a previous use in an infected machine. This compromise could result in manipulated data and could also lead the tallying machine itself to become compromised, exposing the system to future exploits.

Networked data transmission: In tallying setups where votes are tabulated at the polling station and transmitted to the county, or are transmitted from the county to the state through a system other than the election night reporting system, configuration errors in the modem, wifi, or cellular network connections used for transmission can leave the process vulnerable to "man-in-the-middle" attacks. These allow adversaries to manipulate results before they are received at the county (or state) level.

Denial of service: Counties or, where relevant, states, receive results from precinct or centralized counting facilities over the network. Servers can be targeted with a DoS attack by an adversary, resulting in delays in vote reporting during election night.

Recommended actions:

Identify

Know the certification status of all your equipment. The EAC's Voluntary Voting System Guidelines (VVSG) provide federal level certification standards. Many states have their own certification process.

Protect

Vote tallying systems should be isolated from any networks or overall Internet connectivity (commonly referred to as "air-gapped"). This includes connecting to voting machine modems. In the case where you cannot achieve total isolation, restrict network access to precincts and counties to prevent outsiders from accessing or slowing down the system. Again, the best practice is to keep these machines totally isolated and to transfer results to them using removable media as they arrive. As for all removable media, practice the "one-way, one-use" rule.

Use a dedicated single-use system for vote tallying. Using a system solely for vote tallying and disabling unnecessary functionality, like network connection, can limit exposure to attackers.

Require strong passwords and implement two-factor authentication to access the vote tally system device. There are two-factor authentication methods that do not require network connectivity, and that can be implemented.

Use a digital signature to verify the source of vote tallies. Requiring each voting machine to digitally sign its report will prevent a malicious actor from introducing fake results into the tally process.

Keep devices up to date and fully patched. Despite the tally system being air-gapped, it is still important to keep the software on them updated. Review available updates, test how they work with your system, and apply them. You should establish a cut-off date prior to the election after which you will not change the software in order to provide enough time to test the system.

System testing. Include the tallying system in your tests of the system. While conducting penetration tests, teams should look for ways they could access these machines despite the air gap (including testing the physical security) and other ways to force errors in the tallying process.

Detect

Report vote tally totals using multiple forms of communication (redundant communication). For example, electronic vote tally submissions should be confirmed with a follow-up call or text.

Recover

If the electronic system is compromised, implement hand-count procedures.

Vendor Considerations

In many cases, the machines used to tally results will have been provided by vendors who will be involved in the maintenance of those machines. A compromise at this level could cause vote totals to be calculated incorrectly, compromising public trust in the election even if the correct totals are eventually reported.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Election Night Reporting (ENR)

Election night reporting (ENR) consists of the systems and processes for aggregating and communicating the unofficial election results to the public and media after polls close, usually via a website. Counties and states may also report election night results via social media—please see the Internal and Public-facing Communications section for best practice in securing social media accounts. ENR setups vary by state across three principal dimensions defined below:

> **How ENR relates to the vote tallying process**. ENR can be closely linked to the vote tallying process (e.g., a state's non-public vote tallying system might automatically submit results to the state's public ENR website), or can be run separately and in addition to the tallying process.

> **Whether ENR is run by the state, counties, or a combination of both.** Most states run ENR centrally, with counties (or in some cases municipalities) submitting results to the state via a centralized ENR system. In some of these cases, the counties run separate, additional ENR systems (e.g., to provide further granularity on results). In a small number of states, ENR is managed at the county (or municipality) level.

> **Who builds/maintains the ENR system**. Regardless of whether ENR is run at the state or county level, ENR systems can be developed and managed in-house (by the state or county), developed by a vendor but managed in-house, or developed and run by a vendor.

KEY THREATS:

Transmission: In a state-run ENR setup, counties submit their vote reports to the centralized system provided by the state. A configuration error could make this transmission vulnerable to "man-in-the-middle" attacks, where adversaries manipulate vote reports before they are received by the state.

Manipulation of ENR systems: Configuration errors can leave ENR systems vulnerable to exploits or unauthorized access, allowing adversaries to manipulate the vote counts after they have been received in the (state or county) ENR system.

Denial of service: In a state-run ENR set-up, a DoS attack on the transmission of ENR results can lead to a lack of results being reported for one or more counties. In addition, attackers can conduct DoS attacks on the public-facing ENR website, making result reporting unavailable to the public/media altogether during election night.

KEY THREATS (CONTINUED)

Website spoofing: Attackers could redirect public inquiries to a spoofed website, which pretends to be the official ENR system but in reality is controlled by a malicious actor. For example, this could be used in disinformation campaigns to depress voter turnout by saying an election has already been called.

Recommended actions:

Our recommendations should be implemented by the county, state, or external vendor, as appropriate.

Identify

Identify which offices need access to the ENR site or other medium through which they report and consolidate results.

Protect

Require strong passwords and implement two-factor authentication. This should apply to everyone who can access the ENR system.

Secure transmission channels. Require users to authenticate themselves when adding result information and restrict the results they are able to change to only what is within their purview. Ensure all network traffic is secure (e.g., enable SSL on a web-based portal).

Limit access through restricting write privileges for users across the state and counties or within the county as applicable. In state-led ENR systems, specifically ensure that each county can only edit its own vote reports (not those of other counties).

Log incoming election results to help trace and correct inaccurate reports.

Prepare a contingency communications plan for disseminating results if the primary medium is unavailable.

Publicly communicate about ENR process to preempt spoofing. Communicate clearly, ahead of any election, how the state or county will report vote results during election night, to preempt false ENR websites from popping up.

Protect ENR websites against DoS attacks. See Website section for additional recommendations.

Report election night results using multiple forms of communication. They should be confirmed over a second channel; for example, a follow-up call, on top of being sent through the primary channel.

Detect

Each county/precinct should verify that results shown to the public on the official ENR website match the results they reported.

Monitor the ENR system for anomalies in traffic or access during election night. Especially monitor any attempts to change the displayed results (e.g., failed login attempts to the portal) or traffic that may be part of a DoS attack.

Respond and Recover

Public communications around election night reporting are critical. Have a backup plan for how to publicize either that your reporting website is showing no results, or incorrect results. Include the specifics in your communications incident response plan.

Vendor Considerations

Vendors are often responsible for building and/or running both the system for updating results and the webpage that displays those results to the public.

> Be sure that you have an internal (state and local level) backup plan for how to publish results if the vendor system is unavailable.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Internal and Public-facing Communications

Running successful elections requires extensive communication—both within state/county election teams, and with the public. This tends to consist of four key communication channels: internal email communication, official election-related websites, official social media accounts, and the private social media accounts of key officials. All of these communication channels could come under attack by adversaries who abuse them to cause confusion about election logistics before or during election day, and/or to undermine the credibility of the election overall.

INTERNAL COMMUNICATION

Email communication ahead of and during the election is crucial for the election team to coordinate activity internally among states, counties, and precincts/polling stations.

KEY THREATS:

Account compromise: Attackers could compromise key officials' email accounts to send out false information to members of the election team—for example, asking for polling stations to close early or for polling stations to switch to paper pollbooks due to an alleged issue with e-Pollbooks (resulting in delays and lines forming). In addition, compromised accounts could be used to distribute malware across the election team's devices. Clearly, access to the email account of any member of the election team—even at a low level in the organization—exponentially increases the chances of subsequent attacks on the email accounts of more senior members of the election team succeeding.

Recommended action:

Implement two-factor authentication for all official accounts. In most cases, adding a second factor will be enough to prevent an attacker from compromising an account. In addition to this, require strong passwords.

Require all messages to come from official accounts. While officials should take steps to secure their personal accounts as well, all official communication should be done through accounts that have been carefully secured by your IT department.

PUBLIC-FACING COMMUNICATION

Election officials communicate extensively with the public through both ***official election websites*** and ***official social media accounts*** (e.g., Election Board's Twitter account, Secretary of State's official Facebook account). This communication is separate from, and in addition to, election night reporting (which we cover in the section above), and includes, for example, communication to raise awareness of upcoming elections, key deadlines, (e.g., for online registration) and election day logistics (e.g., poll locations, opening hours, ID requirements).

While not officially part of a state's or county's public-facing communication, the ***private social media accounts of key officials*** (e.g., the Secretary of State's private Facebook account) could be used to communicate false election-related information to the public. These should be protected with the same care as the organization's public accounts.

Official Websites

KEY THREATS

Website manipulation (e.g., changing information on polling place location): Malicious actors could look to sow confusion or discourage voters by manipulating the information on official websites. For example, attackers could alter polling site locations and times to make it harder for voters to find their designated vote site

Spoofed websites: To sow distrust in the process, attackers may replicate the official state or county website and post the opposite results than is being reported—for instance the winner of Race A is now the loser.

Distributed denial of service attacks: Similar to voter registration sites, attackers could attempt to shut down official websites on election day to inhibit voters from knowing their designated voting location.

Recommended actions:

Identify

Know who your web hosting provider is and how to contact them.

Determine who is responsible for keeping website software up-to-date.

Know who has the ability to edit your website.

Protect

Have automated procedures to keep software (e.g., Wordpress, Apache) up-to-date. Website software needs to be updated on a regular basis in order to patch vulnerabilities as they are discovered. Have a system for tracking what version of software you are using and what vulnerabilities are discovered and ensure that those vulnerabilities are patched.

Conduct penetration testing and security audits for all resources. Regardless of whether your website was developed by your staff or by vendors, a third-party audit and penetration test can identify vulnerabilities. This should be done anytime a major change is made to website software.

Ensure that developers have been trained on what the common attack vectors are. One good guide for these is the Open Web Application Security Practice (OWASP) Top-10 list.

Ensure sufficient capacity to receive increased site traffic during high-use periods. Provision servers accordingly and conduct load tests ahead of time to be sure that the infrastructure can handle the additional traffic.

Ensure that your website is protected against DDoS attacks and monitor traffic to detect anomalies. Free DDoS protection and mitigation services are available, such as Google's Project Shield and Cloudflare's Athenian Project.

Detect

Have a dedicated person with the job of looking for fake content or spoofed websites in search engine results.

Recover

Have a backup version of the website hosted elsewhere in case the primary site goes down. This version should contain only barebones, essential information (e.g., precinct locations / hours).

Vendor Considerations

Official websites are often created by vendors, and in many cases vendors are also responsible for making changes to them.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Social Media (official and private accounts)

KEY THREATS:

Account compromise: Attackers use spear-phishing to learn the username and password for the county Facebook page which did not have two factor authentication enabled. The attackers then post misinformation about certain voting sites having several hour wait times and direct voters to alternate sites which are then overwhelmed.

Fake accounts: Malicious actors create a fake Twitter account for an election official (e.g., Secretary of State, Election Director) which gains traction because it is retweeted by a bot farm controlling several thousand accounts. The fake account then posts the wrong unofficial election results after polls close.

Recommended actions:

Identify

Be cognizant of which accounts could be used to disseminate information about an election. This includes accounts for your organization, as well as both the professional and personal accounts for officials. Determine who has access to each of these accounts.

Identify points of contact and establish relationships with key social media firms like Facebook and Twitter. Confirm a point of contact in case social media accounts connected to the election are compromised; or in case malicious fake accounts surface. Confirm the requirements for regaining control over accounts and shutting down malicious fake accounts.

Know key stakeholders for communication channels (media, political party contacts, advocacy groups, etc.)

Protect

Inform key officials that their private accounts might be targeted. Establish clear policies for officials and staff on use of private accounts for sharing official information, including policies for communicating indications of malicious cyber activity.

Secure social media accounts. Social media services such as Twitter and Facebook support two-factor authentication for accounts, and enabling this capability is the best step you can take to keep your accounts secure and should be done for both official accounts and the personal accounts of key personnel. In addition to this, require that the passwords for your official accounts be secure.

Understand third-party apps can be a vulnerability if they are compromised. Use third-party social media management platforms judiciously to reduce your threat surface. Periodically review linked accounts and connected apps and remove any that are no longer required.

Detect

Have a dedicated person responsible for looking for fake content in search engine results or on social media.

Recover

See the **Election Cyber Incident Communications Playbook** and **Election Cyber Incident Communications Plan Template** *for State and Local Election Officials*.

Engage with social media firms to recover/disable accounts.

If an account has been compromised, review what permissions it has granted to third-party apps and reset them to prevent further access by unauthorized parties.

Vendor Considerations

If you need to use a third-party social media application to manage social media accounts, then research the applications security practices and access policies to understand what vulnerabilities using it presents.

Vendor Considerations

*(See **Appendix 1, Vendor Selection and Management**, for best practices related to vendor contracts.)*

1. **Clearly define** the division of labor and responsibilities between the vendor and the local officials. Identify any gaps between the two parties and specifically assign responsibility to fill those gaps.
2. **Create and enforce contractual requirements.** Require vendors to adhere to well-defined security practices ensuring safe handling and protection of data.
3. **Require vendor assessments.** State/local contracts with vendors should include provisions requiring vendors to conduct third-party vulnerability assessments of their systems and share the results. See vendor appendix for more details.
4. **Mandate that vendors permit penetration testing of systems**, including voting machines, as part of RFP contracts.
5. **Secure access.** Unnecessary personnel should not have access to systems. Vendors who need access to secure systems should be granted temporary credentials and exercise that access under the supervision of a state or county official. Once a developer has finished building an application, ensure that they do not have access to the production system.
6. **Secure data transmissions.** Require vendor systems to use digital signatures to ensure the integrity of all received and transmitted files.
7. **Require audit logs for any vendor-run system.**
8. **Mandate patching** as part of a vendor request for proposal (RFP) contracts and ensure that the patching is conducted securely and frequently.

Appendices

Appendix 1. **Vendor Selection and Management**

Election system vendors are key partners in addressing cybersecurity risks. Their systems, by definition, increase the attack surface and present additional risk factors that must be mitigated to address cyber threats. Since vendors often develop and maintain systems critical to elections (such as ballot counting equipment and VRDBs), it is crucial to ensure that their protocols and practices meet rigorous cybersecurity standards.

Performing a security risk assessment of vendors during the request for proposal (RFP) process can reveal vendor vulnerabilities and reduce future exposure to external attacks. This risk assessment should be conducted in two steps: 1) during the procurement process, ensure that all vendors are willing and able to comply with security standards that meet, or exceed, election agency expectations, and 2) validate vendors' ability to meet their commitments via thorough due diligence, and ensure that vendors are reviewed periodically, not just at the time of selection.

When assessing a vendor, there are three general principles to consider:

> **Organizational security practices.** Evaluate the extent to which cybersecurity activities and outcomes are embedded across the organization, from the executive level to the implementation/operations level, such as hiring, subcontracting, policies and procedures, cybersecurity awareness and training, network and system management, vendor management, vulnerability management, and software/hardware development.

> **Ongoing partnership capacity.** Vendors should be your partners in addressing cybersecurity risks! Evaluate the levels of transparency associated with their cybersecurity processes, and to what extent they will collaborate with you on key security risk-mitigation activities, including consequence management after a cyber incident. These would include code reviews, vulnerability scans, patching, and implementing controls to strengthen their security posture, while also closing critical gaps.

> **Maintenance strategy.** Cybersecurity is not a "point in time" activity and you may have a long-term relationship with a vendor. As new attacks emerge, software and hardware should be updated commensurate with the nature of evolving risks and the state of the art in cybersecurity safeguards. This expectation must be built into vendor contracts.

Specific security requirements for vendor agreements

With the above principles in mind, security requirements should be clarified in RFPs to ensure that vendors are limiting cyber risks while working with the states or counties. The following set of core security requirements are not exhaustive, but they do provide a foundation to include in vendor RFPs. Each vendor bidder should be required to:

> State how system access in the proposed solution will be managed.

> Describe what type of data will be processed and how it will flow through the system, including any relevant data processing or data storage vendors and, if applicable, locations.

> Describe security at all layers of the solution—application, server, database, data exchange, and network security layers should all have the ability to manage access and privileges at a granular level.

> Describe how security measures will protect data for the entire data life cycle, ensuring that data remains protected for as long as it is in the control of the vendor and, when required, is securely destroyed.

> Describe how the proposed solution meets or exceeds compliance with all state- or county-level security requirements.

> Describe how encryption will be implemented for data "at-rest" and "in-transit."

> Describe how User Access Management will be handled under the principle of "least privilege" (i.e., provide only the minimum level of access required for the user to perform his or her core job), as well as how it will be maintained and pared over time.

> In your Service Level Agreements (SLAs), include clauses for vendors to notify you in the event of a cybersecurity breach of their systems or other unauthorized access immediately after they become aware and to cooperate with any consequential investigation, response, and mitigation.

Transparency requirements should also be established in the RFP to ensure that officials have the ability to perform due diligence and conduct independent security risk assessments. Moreover, transparency will aid in identifying potential conflicts of interest. Non-Disclosure Agreements will protect vendor proprietary information, in exchange for receiving access to:

> **Corporate governance relating to security practices.** Officials should have the ability to review vendors' security policies, standards, and guidelines. They should be able to

assess whether these are implemented in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

Internal security audits. State officials should perform audits (and retain the right to do so) of a vendor's security practices and protocols. This activity provides assurance that the vendor's cybersecurity practices are robust and meet state and local security standards, including those outlined in the above section. This is especially important in the months and years after vendor contracts are signed. Vendor-provided system logs should be contractually viewed as customer owned data not vendor owned data. For instance, voting system audit logs should be readily available to election officials and considered by contract as their data.

Source code. Election officials should have access to the source code for any critical system to perform internal or third-party reviews. This can be a sensitive subject because of intellectual property concerns, but being able to independently audit vendor-created code allows officials to ensure that the code is secure. It also guarantees that the code does not contain any potentially unwanted networking requests, transfers of sensitive information, or modifications to key algorithms and counting mechanisms.

Penetration testing. Penetration testing is a critical element in ensuring that vulnerabilities in vendor environments are proactively identified and closed. The RFP should clearly include requirements for the vendor to allow penetration-testing by state officials or third parties of their systems to discover weaknesses. Vendors may resist these provisions, especially if they hold broader state contracts that could be affected if vulnerabilities are discovered. Nonetheless, conducting these tests represents the best way to identify cracks in critical infrastructure before malicious actors do, and should be part of any contract with vendors who work on and maintain these systems.

Data flow transparency. Officials should have full visibility into data flows for voting system data. Therefore, it is essential for officials to request that the vendor provide its applicable data retention and destruction policies, a list of relevant physical locations where data will be processed, stored, or otherwise accessed, and an exhaustive list of subcontractors who may process, store, or otherwise access voting data or systems. Depending on the nature of the vendor's services, it may be necessary to impose flow-down security and audit requirements on subcontractors, including on the vendor's infrastructure vendors, or, if relevant, to explicitly restrict data storage locations.

Appendix 2. **Election Audits**

While following cybersecurity best practices will help deter and defend against malicious actors, there is no such thing as an impenetrable system. Even if an election system is not attacked, software or hardware errors could lead to an incorrect vote tally. To protect against technical manipulation or failures undermining the process, elections should be "software independent," meaning that they do not rely on a computer to provide a vote count, but instead have an independent auditable paper record for definitive results.

You should conduct a post-election statistical audit with these paper voting records. Such audits provide two critical benefits: (1) they offer transparency and build public confidence in the system and process; (2) they confirm the accuracy of the results, or, on rare occasion, identify that an error has occurred and must be addressed. Post-election audits are designed to be an independent confirmation of the election result. These audits should be observable and reproducible by external third parties. This requires making data necessary to conduct the audit publicly available to independent parties so that they can confirm audit results.

There are two main methods of post-election audits. Since performing a full hand-count of every ballot is extremely time-intensive and the results will likely be inaccurate, other methods are used to inspect the results with a manageable amount of work.

The first audit type uses a fixed percentage of ballots cast. This method, however, can overestimate or underestimate the necessary number of ballots required for a successful audit. In the overestimation case, the audit is inefficient and a waste of resources; in the underestimation case, the audit doesn't fulfill its purpose. That said, a fixed percentage audit is still better than no audit at all and is regarded as a "good" standard of practice.

The second type is the statistical audit where statistical methods are used to determine and inspect the minimum number of ballots required to confirm that an election has not been altered—this would be considered an "enhanced" standard of practice. As the margin of victory between the winner and loser narrows, more ballots are required to ensure an accurate audit. Typical implementations of statistical audits could require multiple rounds of ballot inspection if discrepancies are found with recounted ballots. If the statistical audit fails, a full recount of all ballots is necessary to ensure the election has not been compromised.

The following section discusses the "good" and "enhanced" audit techniques: (1) *Good:* fixed-percentage audits; (2) *Enhanced:* risk-limiting audits with two variants (a) comparison audits, and (b) ballot-polling audits.

Fixed-Percentage Audits

Fixed-percentage audits provide some evidence that results are valid. One example process: Counties indicate to the Secretary of State (or State Election Director) which machines they will use in the election, then the Secretary of State (or Election Director) randomly selects one DRE and one optical ballot scanner per county. The county must then audit a fixed percentage (e.g., 20 percent) of the ballots tallied by the optical scanner, as well as manually counting all the paper vote records produced by the DRE and comparing this number to the DRE's electronic vote count. This process ensures that, for the randomly selected machines, the pre-election logic and accuracy tests were successfully conducted, a chain-of-custody was maintained, and the devices functioned properly on election day. The weakness of a fixed-percentage audit is that specific devices, rather than the election itself, are audited. Election officials cannot be certain that the election as a whole was conducted correctly, but this may be the best available option for some counties with limited resources or technology.

Risk-Limiting Audits (Enhanced Statistical Methods)

The first step in any risk-limiting audit is setting the risk limit. Setting a 5 percent limit means that if an audit is conducted on an election that did, in fact, experience tampering, there is at most a 5 percent chance that the audit will not discover the error and at least a 95 percent chance that the audit will find the election outcome to be manipulated. The number of ballots required for a risk-limiting audit is determined by the risk limit and margin of victory. A closer election or lower limit requires more ballots to be audited. There are two types of risk-limiting audits: (1) comparison audits and (2) ballot-polling audits.

> **A. Comparison vs. Ballot-Polling Audits.** A comparison audit involves recounting a randomly selected set of ballots and comparing those results with the original machine-recorded tabulation of those exact ballots, called the Cast Vote Records (CVRs). Comparison audits are typically recommended over ballot-polling audits for greater efficiency. Unlike a ballot-polling audit, a comparison audit requires knowing the original tabulation results of the specific ballots you are auditing (in the CVR) and comparing

discrepancies. A ballot-polling audit simply looks at the outcome of the ballots inspected. Because of this precision, comparison audits require far fewer ballots to be counted than do ballot-polling audits. However, comparison audits require specific data (machine tabulation and associated paper vote record from a given voting machine), which may be infeasible for some counties.

B. **Audit Level.** Audits can operate on different levels depending on the infrastructure available. A unit could be a single ballot, a batch of ballots, all the ballots processed by a machine or all the ballots in a given precinct. For a given unit, samples are typically selected randomly then the ballots within that unit are inspected. For statistical risk calculations, the larger the unit, the larger the total number of ballots that will need to be inspected to have the same risk of missing an incorrect outcome. Ballot-level comparison audits are most efficient in terms of number of ballots considered for a given margin of victory and risk limit because they spread the audit across many ballots in multiple precincts. This means this audit is more likely to find any election meddling. Batch, machine, or precinct level audits require doing a comparison audit on batches of ballots only at certain precincts. This is less likely to find election meddling and requires auditing more ballots to ensure the same level of confidence that an election outcome is true, but may be more feasible for some counties.

There has been extensive research on this issue by leading experts in the field of election auditing. The following reports can provide additional information:

"A Gentle Introduction to Risk Limiting Audits" Mark Lindeman and Philip B. Stark

"Bayesian Tabulation Audits: Explained and Extended" Ronald L. Rivest

"On the Notion of 'Software-Independence' in Voting Systems" Ronald L. Rivest and J.P. Wack

"Evidence-Based Elections" by Philip B. Stark and D.A. Wagner

External Resources Guide

There are many threats that could undermine the democratic process; fortunately, election officials are not in this alone. There are resources available that can help defend against those threats, including free ones.

Federal Support

The Department of Homeland Security (DHS) Office of Cybersecurity and Communications (CS&C) offers a variety of services at no cost or minimal cost for states and counties. Services include:

1. Cyber Hygiene checks, which scan election and other Internet-accessible systems (such as public-facing VRDB portals) for vulnerabilities and configuration errors. DHS can also provide a report that outlines steps to address or mitigate vulnerabilities detected in the scan.
2. Risk and Vulnerability Assessments (RVAs), which involve DHS teams performing in-depth on-site analysis of a state or local election facility's internal and external networks. RVAs can include penetration testing, vulnerability scanning and testing, database and operating systems scans, Web application scanning and testing, and several other services.
3. The National Cybersecurity and Communications Integration Center (NCCIC) is a cybersecurity situational awareness, incident response, and management center that operates 24 hours a day, 7 days a week. NCCIC collaborates with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide information to State and local governments.
4. MS-ISAC disseminates early warnings on cyber threats to state and local governments as well as security incident information and analysis through a 24-hour security operations center. MS-ISAC also provides intrusion detection.
5. Cyber Security Advisors (CSA) and Protective Security Advisors (PSA) are security professionals deployed in all 50 states to provide direct assistance, such as vulnerability assessments, and reach-back to additional government resources and capabilities.

Private Sector Support

For defending election system-related public-facing websites, Google's Project Shield and Cloudflare's Athenian Project are free services that defend websites from distributed denial of service (DDoS) attacks. Other software development firms are developing free open source software to assist states and localities in conducting risk-limiting audits. Several highly experienced cybersecurity firms also offer penetration testing and risk vulnerability assessments.

National Guard Collaboration

The National Guard is building cyber units in many states and territories. These units align with the Army and Air Force. When not performing their federal mission, these units may be available for state-specific tasking under state authorities. Several states have employed their National Guard cyber capabilities to participate in activities such as vulnerability assessments and penetration testing.

Recognizing that there are Constitutional and legal sensitivities, states interested in exploring opportunities with their National Guard units should work through their governor's office and ultimately their state's Adjutant General office. If states do not have a resident National Guard cyber capability, they can potentially partner for support with nearby states who do have this resource. In some cases, support can be provided through the Emergency Management Assistance Compact (EMAC) process, similar to other civil support capabilities. These compacts act as a complement to the federal disaster response system, providing timely and cost-effective relief to states requesting assistance. A useful analogy is to consider National Guard support in cyberspace in a similar light as the laying of sandbags before a storm in the physical world.

What Every Election Staffer Should Know About Cybersecurity

1. **Everyone is a security official**
   Take cybersecurity seriously. Take responsibility for reducing risk, training your staff, and setting the example. Human error is the number one cause of breaches. Spear-phishing attacks and other attempts at interference can be thwarted with cybersecurity vigilance.

2. **Use two-factor authentication (2FA)**
   Use two-factor authentication for everything: official work accounts, personal email accounts, social media accounts, and any data storage services. Use a mobile app (such as Google Authenticator, Duo, or Authy) or a physical key (such as Yubikey or other U2F devices) for your second factor, not text messaging. 2FA is an extra step, but is very effective at preventing unauthorized access.

3. **Create long, strong passwords**
   Current computing capabilities can crack a seven-character password in milliseconds. For your passwords, create **`SomethingReallyLongLikeThisString`**, not something really short like **`Th1$`**. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with lots of **`$ymB01$`**.

4. **Keep credentials secure**
   When collaborating with others, resist the temptation to share credentials to systems with them, regardless of who they are.

5. **Practice cyber hygiene**
   Follow all applicable guidance for patching and software updates. Ensure that your systems have the most updated antivirus software.

Glossary

Based on the Election Assistance Commission's Common Cybersecurity Terminology and Information Technology Terminology Glossaries

Cybersecurity Terms:

Access
Ability to make use of any information system (IS) resource.

Access control
The process of granting or denying specific requests: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities.

Advanced Persistent Threat
An adversary who possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Air gap
An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).

Asset
A major application, general support system, high impact program, physical plan, mission-critical system, personnel, equipment, or a logically related group of systems.

Attack
An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.

Attacker
A party who acts with malicious intent to compromise an information system.

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Backups
A copy of files and programs made to facilitate recovery if necessary.

Black-box testing
A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as basic testing.

Blacklist
A list of entities that are blocked or denied privileges or access.

Breach
Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected information.

Compromise
A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information has occurred.

Critical infrastructure
System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, economic security, national public health or safety, or any combination of those matters.

Cybersecurity
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Data Loss
The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Decryption
The process of changing ciphertext into plain text using a cryptographic algorithm and key.

Denial of Service
The prevention of authorized access to resources or the delating of time-critical operations.

Encryption
The process of encoding messages or information in such a way that only authorized parties (or software applications) can read it. Encryption does not prevent interception, but denies the message content to the interceptor. Encrypted information must be decrypted before it can be rendered into plain text or other usable format. Encryption and decryption add overhead to processing and can slow systems down. Voting systems will commonly encrypt data within a voting system component before transmitting it to another device.

Firewall
The process integrated with a computer operating system that detects and prevents undesirable applications and remote users from accessing or performing operations on a secure computer.

Hack
Unauthorized attempt or access to an information system.

Hash Function
An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message, and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message.

Incident Response Plan
The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attack against an organization's information systems(s).

Intrusion
A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Multi-factor Authentication
Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something that identifies who you are (e.g., biometric).

Password
A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Patch
An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Penetration Testing
Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Phishing
Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Port
The entry or exit point from a computer for connecting communications or peripheral devices.

Port scanning
Using a program to remotely determine which ports on a system are open (e.g., whether the systems allow connections through those ports).

Private key
A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm. For digital signatures, the private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key or to decrypt information which has been encrypted using the public key.

Risk analysis
The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

Risk assessment
The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls that are planned or in place.

Spear Phishing
A colloquial term that can be used to describe any highly targeted phishing attack.

Spoofing
Faking the sending address of a transmission to gain illegal entry into a secure system.

Structured Query Language (SQL) injection
An attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code.

Supply Chain
A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

Tabletop Exercise
A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Threat
Any circumstance or event with the potential to adversely impact organizational operations, (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Trojan horse
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Unauthorized access
Any access that violates the stated security policy.

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Whitelist
A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline.

General Information Technology Terms:

Air Gap

An air gap is a physical separation between systems that requires data to be moved by some external, manual procedure. Also called "Sneaker Net." Election systems often use air gaps intentionally to prevent or control access to a system. Copying election results to a CD or USB drive, then walking that media to a different computer for upload and use in a different system is an example of an air gap.

Audit

A review of a system and its controls to determine its operational status and the accuracy of its outputs. Election system audits seek to determine if controls are properly designed and functioning to ensure the correctness of intermediate and final results of the system's processing.

Audit trail

The records that document transactions and other events. Some audit trails in election systems are event logs, paper records, error messages, and reports.

Authentication

The process of identifying a user, usually by means of a username and password combination. Election systems use authentication methods to assure that only those users with appropriate authority are permitted access to the system. Authentication schemes should not permit group logins.

Blacklist

A list of URLs, domains, users, or other identifiers, that have had system access or privileges blocked. Election offices may wish to "add" domains to be blocked to a blacklist, maintained by their system administrator.

Code

n. Synonym for program or software.

v. to create or modify software.

Data destruction

The removal of data from a storage medium. Election officials should destruct all data on election systems before selling or disposing of the systems. Any election system that is to be destroyed should use a reputable company and best practices for destruction, so that data cannot be obtained after it is no longer in the custody of the election official.

Database
A structured collection of data that includes data and metadata (data about the data). Databases are managed by database management systems. The election database stores all of the requisite information to manage election including precinct information, race and candidate information, and data used to prepare the ballots, tabulate, and report results.

Download
Transferring data from a larger computer to a smaller computer or device. An EMS facilitates downloading ballot images to vote capture devices.

Dox
Publish damaging or defamatory information about an individual or organization on the Internet. One method of hacking a campaign is doxing (or doxxing).

File
A collection of related data, stored on media. Files will be identified by a system-valid filename.

Firewall
A gateway computer and its software that protects a network by filtering the traffic that passes through it. Election offices often need to reconfigure the firewall to permit large files or complex files to be passed through the firewall that separates the office from the Internet.

Two-factor Authentication
Authentication mechanism requiring two or more of the following: something you know (e.g., Password), something you have (e.g., Token), something that identifies who you are (e.g., biometrics).

Penetration Testing
Also called Pen Testing. An evaluation method that enables a researcher to search for vulnerabilities in a system. Election systems, such as the VR system, are periodically submitted to a Pen Test to determine their vulnerabilities to cyber attacks.

Ransomware
Malware that holds the victim's device (computer, phone, etc.) and data for ransom, by means of encrypting the files on the device or preventing access to the device. Election office computers should maintain high levels of cyber hygiene, including up-to-date anti- malware systems and adherence to best practices regarding managing browser and email client activities.

Social Engineering
Misleading users into providing information that can be used to compromise the security of a system. Usually low-tech. Social engineering of election officials includes emails and phone calls requesting information that can be used to spoof accounts or hack passwords.

Software
A synonym for program. Computer software is the collection of programs that control the computer and perform a specific collection of tasks. Software has version numbers and is licensed (not sold) to the end user. Software can be altered to change the functionality of the computer. The Election Management System (EMS) used to create election databases is software.

Spear Phishing
A targeted attack by hackers, via bogus emails, that attempts to get the victim to provide login information or personal information to the hackers. Spear Phishing attempts may appear to originate from legitimate, known sources, such as organizational IT or known vendors. Election officials should NOT click through on suspicious links or open attachments without first verifying that the email is legitimate.

Software Patches
Also called fixes or bug fixes. Corrections to existing programs, designed to be integrated into the programs without major release changes. Patches or fixes to voting systems must be tested before being applied, and may invalidate certifications. Do not install software patches without extensive technical review for unintended consequence.

Tabletop Exercise
A discussion-based drill where qualified personnel discuss scenarios and responses in order to validate plans and procedures. Also called Incident Response Planning. Election officials exchange in tabletop exercises to determine the viability of their election continuity plans.

Wi-Fi
Wi-Fi is a wireless networking technology that uses radio waves to provide wireless high- speed Internet and network connections. Wi-Fi is a trademarked phrase for the *IEEE 802.11x* standard. Wireless is less secure than Ethernet connections. Some e-Pollbook and voting system technologies use Wi-Fi or wireless connectivity at the polling place.

Election Administration Technology Terms:

Central Count Optical Scan
Optical scan system that utilizes one or more high-speed scanners at a central location to tabulate ballots. Central count systems are usually paired with Vote By Mail technologies. Central count systems lack overvote/undervote protection capabilities.

Digital Optical Scan System
Optical scan system that converts voter choices on a paper ballot to digital values. Digital op scan systems can accommodate a broader range of paper types, sizes of paper, ballot layout, and voter marks than IR op scan systems.

Direct Record Electronic Voting System (DRE)
A DRE system presents a ballot image to a voter, collects the voter's choices, and records those choices directly onto electronic media. DREs may be fitted with VVPAT subsystems to create a paper artifact of the voting transaction. DREs are capable of audio interaction and image displays, and can hold a large number of ballot styles in multiple languages.

Election Night Reporting Systems (ENR)
A web-based system that aggregates and displays unofficial election results across the jurisdiction. ENR systems can be real-time or near-real-time, and acquire their data from the EMS. ENR systems can provide multiple formats for displaying election results and may provide direct feeds for the media.

Electronic Poll Book (EPB)
Hardware and/or software that permits election officials to review the electors list and mark voters who have been issued a ballot. Also called an e-Pollbook. E-Pollbooks can be standalone at the precinct with a separate copy of the electors list, or can be networked into a central voter registration system and check and update voter records in real time.

High-Speed Central Count Tabulation System
An optical scanner capable of scanning a high number of ballots (hundreds) per minute. These large and complex scanners are typically used in vote-by- mail jurisdictions, in large jurisdictions that have a large number of absentee ballots, or in central count jurisdictions.

Optical Scan System (Op Scan)
A voting system that can scan paper ballots and tally votes. Most older op scan systems use Infrared (IR) scanning technology and ballots with timing marks to accurately scan the ballot.

Precinct Count Optical Scan
Optical scan technology that permits voters to mark their paper ballots within a precinct and submit the ballot for tabulation. Precinct Count systems provide overvote/undervote protection.

Risk-Limiting Audit
Risk-limiting audits provide statistical assurance that election outcomes are correct by manually examining portions of paper ballots or voter-verifiable paper records.

Voluntary Voting System Guidelines (VVSG)

Collection of standards that is developed and maintained by the EAC. The VVSG specifies a minimum set of performance requirements that

Voter Verified Paper Audit Trail (VVPAT)

Contemporaneous paper-based printout of voter choices on a DRE.

Do you see a way to make this Playbook better?

Are there new technologies or vulnerabilities we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #electionplaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Copyright 2018, President and Fellows of Harvard College

Illustration icons from the Noto Emoji project, licensed under Apache 2.0.

National Association of Elections Officials
Election Center
Elections Security Checklist

May 2017

10

ELECTION CENTER

21946 Royal Montreal Drive, Suite 100, Katy, TX 77450 281-396-4309

Elections Security Checklist

Identify and Assess Critical Election Systems	
1.) Have you defined your inventory of critical election systems? *(for example, the Voter Registration Database; Websites like your Voter Data Lookup Tool; Election Tally System; Voting Machines, etc.)*	❑ YES ❑ NO
2.) For each system, do you regularly assess the value of the information contained within, the necessity of perfect functioning of the system, and potential risks to it?	❑ YES ❑ NO
3.) For each system, are you actively cataloging it and building/improving defenses to protect it?	❑ YES ❑ NO
4.) For each system, have you developed a plan to recover should disaster strike?	❑ YES ❑ NO
For each system identified, engage in the following critical analysis to assess the relative risks, defenses, and recovery plans you have in place.	
I. Risk Assessment **(Complete a Risk Assessment for every system)**	
A. Physical Security Risk	
1.) Have you developed a worst case scenario for potential damage if an unauthorized person enters your election headquarters?	❑ YES ❑ NO
2.) Have you developed a worst case scenario for potential damage if an unauthorized person enters your election warehouse?	❑ YES ❑ NO
3.) Have you developed a worst case scenario for potential damage if an unauthorized person enters your server room or data center?	❑ YES ❑ NO
4.) Have you examined your physical access authorization policy in the last three months?	❑ YES ❑ NO
5.) Do you perform scheduled audits of authorized personnel prior to each election?	❑ YES ❑ NO
6.) Do you reexamine your physical access policies on any regular schedule?	❑ YES ❑ NO

© Copyrighted by the Election Center
Reprint only with permission of the Election Center

A. Physical Security Risk (con't)	
7.) Have you ever conducted a test to see if your facilities can be entered by unauthorized personnel?	❑ YES ❑ NO
8.) Do you have policies and procedures in place for intrusion incident response?	❑ YES ❑ NO
9.) Do you have surveillance cameras in place at key facilities?	❑ YES ❑ NO
10.) Do you have a system in place that automatically identifies suspicious behavior as seen on the surveillance system and creates a management alert?	❑ YES ❑ NO
11.) Do you regularly review your video if there is not a system to automatically identify suspicious behavior?	❑ YES ❑ NO
B. Network Security Risks	
1.) Do you have a complete map of your network and all its interconnections, both within your organization and with outside entities?	❑ YES ❑ NO
2.) Do your vendors and partners have a strong commitment to network security?	❑ YES ❑ NO
3.) Have you reviewed your vendors and partners' written plans and checkpoints that demonstrate implementation?"	❑ YES ❑ NO
4.) Do you have a map of the data elements that pass between each application system on your network and with outside entities?	❑ YES ❑ NO
5.) Are all of your network connections to outside entities secured by a Virtual Private Network (VPN) or something comparable?	❑ YES ❑ NO
6.) Is there any group or department within your organization whose mission is to monitor network security?	❑ YES ❑ NO
7.) Have you developed a worst case scenario for potential damage if an unauthorized person gains access to any part of your network?	❑ YES ❑ NO
8.) Do you have anti-virus software installed to detect "Advanced Persistent Threats"?	❑ YES ❑ NO
9.) Does any outside entity, such as a statewide voter registration system, have the ability to alter or delete data from any of your internal systems?	❑ YES ❑ NO
10.) Do you regularly conduct vulnerability and intrusion testing on your network?	❑ YES ❑ NO

© Copyrighted by the Election Center
Reprint only with permission of the Election Center

C. Software Applications Security Risks *(Note: Systems may have numerous applications that touch them. For example, a voter registration system may be composed of a voter database application, and also connected e-poll book software application, and connected statewide voter database application. Running the application level analysis on each of the program level applications will give you your best sense of your security and preparedness.)*	
1.) Application (insert name) Security Risks (repeat a, b, c and d questions for every security risk application)	
a.) Information at Risk	
1.) Does your application house any information not subject to public disclosure? *(for example, any personally identifiable information (PII) such as SSN, Driver's license, date of birth, etc.)*	❑ YES ❑ NO
2.) Do you employ encryption standards for all data - specifically personal identifiable Information?	❑ YES ❑ NO
3.) Does this application share, transmit, or receive information with any other application or system?	❑ YES ❑ NO
4.) Does this application house any data that affects election results?	❑ YES ❑ NO
5.) Does this application have any type of network or internal system connection with any application that affects election results?	❑ YES ❑ NO
6.) Does this application house any data that is essential to the running of an election, and without which the election would either be impossible to administer or whose results might be questioned?	❑ YES ❑ NO
b.) Acceptable Use Policy	
1.) Do you have a written policy for this application describing who may use it and under what circumstances?	❑ YES ❑ NO
2.) Do you have an enforcement mechanism and management review process in place to ensure compliance with any such policy?	❑ YES ❑ NO
3.) Is your acceptable use policy implemented in software in such a manner that your systems enforce the policy?	❑ YES ❑ NO
c.) Worst Case Scenarios	
1.) If this application or its database were completely destroyed or disabled at a critical time, could you still conduct your election?	❑ YES ❑ NO

© Copyrighted by the Election Center
Reprint only with permission of the Election Center

c.) Worst Case Scenarios (con't)	
2.) Even if you could conduct the election, would public confidence in the results be maintained? *(for example, a hacker had cancelled a large number of voter registrations for one competing party)*.	❑ YES ❑ NO
3.) Could you still ensure that no voters would be disenfranchised as a result of the application problem? *(for example, excessively long lines, or unavailable registration information, or for some other reasons)*.	❑ YES ❑ NO
II. Defense Layers	
A. Physical Defenses	
1.) Is physical access to your site restricted to authorized users?	❑ YES ❑ NO
2.) Is there site security staff at the location(s) where your system is located?	❑ YES ❑ NO
3.) Is there a log of the identities and access times of individuals physically accessing your site?	❑ YES ❑ NO
4.) Is your site security staff present at times when staff are not present?	❑ YES ❑ NO
5.) Are all entrances (including windows, etc.) secured by alarms and/or security cameras?	❑ YES ❑ NO
6.) Does your management regularly review physical security records such as logs, video footage, alarm notifications, etc.?	❑ YES ❑ NO
7.) Is the data center where your computer servers are located physically protected in the event of fire, terror attacks or flooding?	❑ YES ❑ NO
8.) Do you have a backup site available if any of your facilities become suddenly inoperable during a critical period?	❑ YES ❑ NO
9.) Have you determined how long it will take to get the backup site functioning? (including the determination of any loss of data).	❑ YES ❑ NO
10.) If any of your computer systems are housed in a vendor-supported data center, has that vendor supplied you with a detailed description of their physical security, fire protection, backup and recovery procedures?	❑ YES ❑ NO
11.) Are your temporary workers required to wear ID badges or other identification so that unauthorized persons in your facilities can be quickly spotted?	❑ YES ❑ NO

© Copyrighted by the Election Center
Reprint only with permission of the Election Center

B. Network Defenses	
1.) Is there an "air gap" between the Internet and your election tally system *(i.e. is your tally system physically disconnected from the Internet)*?	❑ YES ❑ NO
2.) Do you employ encryption standards for all data - specifically personal identifiable Information?	❑ YES ❑ NO
3.) Are your public-facing voter systems, e.g. a "check my registration" application, built using copies of critical information rather than being directly connected to critical information databases?	❑ YES ❑ NO
4.) Do you review your network activity logs daily?	❑ YES ❑ NO
5.) Do you review your logs at least once a week?	❑ YES ❑ NO
6.) Do you have any User & Entity Behavior Analytics (UEBA) software running on any of your critical infrastructure that can alert you to suspicious network activity?	❑ YES ❑ NO
7.) Do you conduct any periodic vulnerability, intrusion and penetration testing on your networks?	❑ YES ❑ NO
8.) Do you create and store daily application system back-ups?	❑ YES ❑ NO
9.) Do you transfer data to or from the isolated network using a specified USB device that is used only for that purpose and verified to be clean?	❑ YES ❑ NO
10.) Do you have a network access control system that controls user access permission levels? *(e.g. Microsoft Active Directory)*	❑ YES ❑ NO
11.) Do you control access to any of your systems by outside organizations or individuals by using Virtual Private Networks (VPNs)?	❑ YES ❑ NO
12.) Is your network password-protected?	❑ YES ❑ NO
13.) Do you provide administrative passwords only to employees with a clearly defined "need to know/edit" status?	❑ YES ❑ NO
14.) Do you change critical system passwords regularly *(recommendation every 90 days)*?	❑ YES ❑ NO
15.) Do you ensure that servers, PCs and laptops are encrypted or updated with the most current security patches?	❑ YES ❑ NO
16.) Do you ensure the organization has the most current versions of virus protection software?	❑ YES ❑ NO

© Copyrighted by the Election Center
Reprint only with permission of the Election Center

C. Software Applications Defenses	
1.) Application (insert name) Defenses **(repeat a., b., c., d questions for every software defense application)**	
a.) Data Protections	
1.) Are only authorized personnel granted access to the software?	❑ YES ❑ NO
2.) Is this application set up with different, unique passwords for each user?	❑ YES ❑ NO
3.) Is this application set up with different passwords for different elections?	❑ YES ❑ NO
4.) Is this application set up with robust passwords *(passwords include special characters and caps-best practices recommends changing passwords every 90 days)*?	❑ YES ❑ NO
5.) Is this application set up with tokens or other special access rights?	❑ YES ❑ NO
b.) Software level application level protections	
1.) Is the software platform protected by a firewall?	❑ YES ❑ NO
2.) Is the software platform isolated in the network environment?	❑ YES ❑ NO
c.) Software Logs	
1.) Does the software log the user name, time, date, and type of modification?	❑ YES ❑ NO
2.) Does the software log multiple log-in attempts, increased data traffic, and/or volume of data transmitted?	❑ YES ❑ NO
d.) User & Entity Behavior Analytics (EUBA)	
1.) Do you have baseline measurements for “normal” activity patterns within this application and an alert system that identifies abnormal activity patterns?	❑ YES ❑ NO
III. System Disaster Recovery	
A. Physical Disaster Recovery	
1.) Is there backup for the loss of hardware *(networks, servers, computers and laptops, wireless devices)*?	❑ YES ❑ NO
2.) Is hardware available at an alternate facility that can be configured to run similar hardware and software applications when needed?	❑ YES ❑ NO
3.) Is there backup for the loss of impounded voting equipment?	❑ YES ❑ NO

© Copyrighted by the Election Center
Reprint only with permission of the Election Center

A. Physical Disaster Recovery (con't)	
4.) Is there a contingency for natural disasters or homeland security breach for data contained at data center?	❑ YES ❑ NO
5.) Are there plans for relocating Receiving Stations (where poll workers return election night supplies) in the event of a natural disaster or homeland security breach?	❑ YES ❑ NO
6.) Is there backup for the loss of data from election equipment damage?	❑ YES ❑ NO
7.) Is there access to network infrastructure hardware that could replace failed components?	❑ YES ❑ NO
8.) Is there ready access to your alternative physical locations?	❑ YES ❑ NO
9.) Is there a timeframe in place for the alternative facility to be functioning?	❑ YES ❑ NO
B. Network Disaster Recovery	
1.) Is there a plan for providing automatic redirects for interfaced systems should you need to move your system to a new network location?	❑ YES ❑ NO
2.) Is there access to network infrastructure hardware that could replace failed components?	❑ YES ❑ NO
3.) For the backup hardware and networking plan, is there necessary staff available during critical periods?	❑ YES ❑ NO
C. Software Applications Disaster Recovery	
1.) Application (insert name) Disaster Recovery **(repeat a., b., c., d questions for each software disaster application)**	
a.) Damage Assessment	
1.) Are vendors on standby for critical periods to assist with Assessment and Disaster Recovery?	❑ YES ❑ NO
2.) Are you able to run a hash comparison with the recovery (i.e. back-up) copy of your software application?	❑ YES ❑ NO
b.) Data Restore	
1.) Are your backup disks or file locations readily accessible?	❑ YES ❑ NO
2.) Are your backup files saved in an off-site location?	❑ YES ❑ NO
3.) If you have a parallel application running, is it up to date?	❑ YES ❑ NO

© Copyrighted by the Election Center
Reprint only with permission of the Election Center

c.) Application Restore	
1.) Do you have necessary staff or vendor resources available to assist with the installation of the application in a mirrored physical and OS environment?	❑ YES ❑ NO
d.) Business Restore	
1.) Are you prepared to cut over to alternative applications that can manage limited business critical functions? *(For example, if your Voter Registration System crashes, can you quickly utilize your web based voter search application so that you can direct voters to their polling place on Election Day?)*	❑ YES ❑ NO
2.) Are there paper alternatives to allow you to continue with on-going critical processes while technical systems are diagnosed and brought back? *(For instance, do your voting machines create countable paper trails viewable by each voter?)*	❑ YES ❑ NO
3.) Can you quickly create paper voter lists in the event e-poll books go down?	❑ YES ❑ NO
The Election Center would like to acknowledge and thank the committee that worked on the initial draft of this checklist: Noah Praetz, Cook Co. IL; Dean Logan, Los Angeles Co. CA; Jennifer Morrell, Arapahoe Co. CO; Janice Case, King County, WA; Eric Fey, St. Louis Co. MO; Brian Corley, Pasco Co, FL and Ryan Macias, U.S. EAC	

© Copyrighted by the Election Center
Reprint only with permission of the Election Center

Voting System Technical Oversight Program at Ball State University (VSTOP)

Indiana Best Practices Manual for the Operation of Election Equipment

June 2018

Indiana Best Practices Manual for the Operation of Election Equipment

JUNE 25, 2018

Voting System Technical Oversight Program

VSTOP

Indiana Best Practices Manual for the Operation of Election Equipment

Prepared by
Voting System Technical Oversight Program
(VSTOP)
Bowen Center for Public Affairs
Ball State University

Version 1.1
June 2018

Version History

Date	Version Number	Description
March 28, 2018	1.0	Original draft version
June 4, 2018	1.0	Revised draft version
June 25, 2018	1.1	Revised

Table of Contents

1. Introduction
2. Best Practices for the Operation of Voting Systems
3. Best Practices for the Operation of Electronic Poll Books
4. Election Cybersecurity Best Practices
5. Election Physical Security Best Practices
6. Standards and Best Practices based on Indiana Election Code
7. Resources
8. Glossary

1. Introduction

Since the Help America Vote Act (HAVA) was passed by the United States Congress in 2002, Elections and Voting Systems have changed considerably. Today's voting systems are totally dependent on Information Technology and, according to the United States Election Assistance Commission (EAC) publication *Ten Things to Know About Selecting a Voting System*, *Managing Election Technology Series #1* [1], the "Election Official of today is an Information Technology (IT) Manager."

IC 3-5-2-53 incorporates this definition of voting system as follows:

IC 3-5-2-53 "Voting system"
Sec. 53. "Voting system" means, as provided in 52 U.S.C. 21081:

(1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support that equipment) that is used:
- (A) to define ballots;
- (B) to cast and count votes;
- (C) to report or display election results; and
- (D) to maintain and produce any audit trail information; and

(2) the practices and associated documentation used:
- (A) to identify system components and versions of those components;
- (B) to test the system during its development and maintenance;
- (C) to maintain records of system errors and defects;
- (D) to determine specific system changes to be made to a system after the initial qualification of the system; and
- (E) to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

As added by P.L.4-1991, SEC.5. Amended by P.L.209-2003, SEC.3; P.L.164-2006, SEC.2; P.L.128-2015, SEC.5.

Additionally, HAVA also established the EAC and prescribed the development of Voluntary Voting System Guidelines (VVSG) to help the States test, certify and implement voting system hardware and software. The State of Indiana requires, among other conditions, that voting systems certified in the state be VVSG compliant. The Voting System Technical Oversight Program (VSTOP) works with the state to manage the testing and certification of voting systems. VSTOP has also developed the "Indiana Electronic Poll Book (ePB) Certification Test Protocol" [2] for certification and testing of electronic poll books (ePBs) used in Indiana.

This **Indiana Best Practices Manual for the Operation of Election Equipment ("Manual"**) has been designed with you, the County level election official, in mind. This Manual will also be useful to poll workers and other involved in conducting elections. VSTOP's goal in bringing this manual to you is to provide a collection of the current set of best practices in the operation of voting systems, ePBs, cybersecurity, and physical security of election equipment and materials.

The scope of this Manual is limited to the collection of best practices described above. This Manual is not designed to replace the operations manuals of your county's voting systems and/or electronic poll books. Rather, this Manual is a set of general best practices that apply to all types of voting equipment (including electronic poll books). These best practices are in addition to the best

practices that may be included in the operating and training materials that came with your election equipment.

This Manual includes the following Sections.

The section on *Best Practices for the Operation of Voting Systems* includes general best practices that apply to any type of voting system and associated equipment and materials.

The section on *Best Practices for the Operation of Electronic Poll Books* includes general best practices that apply to ePBs and their functionality.

The section on *Election Cybersecurity Best Practices* covers cybersecurity related best practices that apply to all aspects of conducting elections, including the use of voting equipment, while the section on *Elections Physical Security Best Practices* covers similar aspects for physical security of election equipment and related materials and resources.

The section on *Standards and Best Practices based on Indiana Election Code* includes a discussion of Indiana statutes that apply to physical and cybersecurity aspects of elections and election equipment. This section may be expanded in future versions to include similar federal election statutes.

VSTOP has consulted many resources to compile the information in this Manual. These resources include the National Institute of Standards and Technology (NIST), The Belfer Center, Harvard Kennedy School, U.S. Election Assistance Commission, National Conference of State Legislatures (NCSL), and the Indiana Department of Homeland Security.

A complete list of those resources is included in the *Resources* section. We recommend that you consult these resources as often as needed and check these regularly since new information is regularly added. Hyperlinks are provided where available.

The Manual concludes with a *Glossary* and a set of *End Not*es that include the collection of references used in this Manual.

It is our expectation that this Manual will undergo frequent revisions and updates. We expect to provide the most recent version in a downloadable format. For more information please contact the VSTOP Team at vstop@bsu.edu.

We value your questions, feedback and suggestions for changes and additions. Those will help us improve future versions of the Manual. Please write to us at vstop@bsu.edu.

2. Best Practices for the Operation of Voting Systems

This section presents best practices for voting system operation. These best practices apply to all voting systems and are not vendor specific. We group the best practices into several categories.

Best Practices for Keeping your Voting System Up-To-Date:

- Know the certification status of all your voting system equipment (this may be done by referring to your inventory in the VSTOP-ESI inventory database or by referencing similar information on the IED/SOS website).
- Monitor technical bulletins from your vendor. Ask your vendor about any known or new issues.
- Monitor changes to your voting system such as modifications and engineering change orders (ECOs). You may ask your vendor about any changes, contact VSTOP for the information or refer to the VSTOP-ESI inventory database.
- Follow your vendor's manuals and best practices for voting system operation.
- Keep a record of your voting system's maintenance.
- Follow your vendor's guidelines for environmental requirements for storage and transportation of voting equipment and peripherals/accessories.

Best Practices for Aging Voting Systems: The EAC publication, 10 Things to Know About Managing Aging Voting Systems, *Managing Election Technology Series #2"* [1] discusses the issue of aging voting systems. After the passage of HAVA, as the article mentions, there was a surge of voting system acquisitions across the country in the years 2002 to 2005. With rapid changes in technology, funding limitations, and increasing requirements about security, jurisdictions have to find ways to extend the life of some of these older systems. The EAC publication includes the following:

- Maintain a spreadsheet that includes the serial number for each voting system and ePollbook to record any issues with the equipment and the resolution.
- As you prepare for elections, run a stress test on the power supply and check all batteries that are used in the voting systems and their components.
- Watch for wear-and-tear of non-technical parts and repair or replace as necessary. Examples include Velcro strips, loose screws, and small washers and nuts.
- Monitor Technical Bulletins from your vendor for modifications, Engineering Change Orders (ECOs), end-of-life (EOL) components and related issues.
- Network with other election officials in the State using the same voting equipment.
- Evaluate your poll worker training materials after each election. Assess your poll workers' learning.
- Conduct Logic & Accuracy testing of your voting systems before the required public test of voting systems. This pre-test will confirm if the voting system's tabulation matches the expected results from a pre-audited set of ballots. Any identified issues in the pre-test can be corrected before the public test.

Best Practices for Voting System Access: Both physical and cyber security are enhanced when an organization has well defined policies on who has access to the system. This includes both physical access to storage locations, and access to the systems and equipment. You must control and actively monitor access. The Belfer Center Report [5] includes several best practices for access control.

- Limit the number of people with access to the system to those who need it to complete their jobs (the "who"). [5] p.16
- Restrict what each user is authorized to do. [5] p.16
- Quickly remove those who no longer need access. [5] p.16

- Keep a list of all users who have access and their access levels.
- Regularly adjust access and permissions as personnel change. [5] p.19

Best Practices for Removable Media:

- Restrict the use of removable media devices (for example, USB/thumb drives, compact discs, memory cards) with voting systems. [5] p. 17
- Use only media that is approved/certified for use. Make sure you have back-up in the event of equipment failure. Know where to acquire/purchase removable media in the event yours becomes damaged.
- Limit the use of removable media only to voting systems.
- Scan media devices for malware. [5] p. 34
- When data on removable media is no longer needed, erase and reformat.
- Treat all removable media as a potential delivery mechanism for malware. Institute a "one-way, one-use policy: "only use physical media once, from one system to a second system, then securely dispose of it." [5] p. 20
- Keep an inventory and a chain of custody/tracking system for all removable media.

3. **Best Practices for the Operation of Electronic Poll Books**

Many of the best practices for voting systems also apply equally well to electronic poll books (ePBs). This section presents best practices for ePB operation. These best practices apply to all ePBs and are not vendor specific. We group the best practices into several categories.

Best Practices for Keeping your Electronic Poll Book Up-To-Date:

- Know the certification status of all your ePB equipment by consulting the VSTOP-ESI database or the IED/SOS website.
- Monitor technical bulletins from your vendor. Ask your vendor about any known or new issues.
- Ensure all devices are updated and patched. Test the electronic poll book to ensure that it is fully functional after patches have been applied.
- Monitor changes to your ePB such as modifications and engineering change orders. You may ask your vendor about any changes, contact VSTOP for the information or refer to the VSTOP-ESI inventory database.
- Follow your vendor's manuals and best practices for ePB operation.
- Keep a record of your ePB's maintenance.
- Follow your vendor's guidelines for environmental requirements for storage and transportation of your ePBs and peripherals/accessories.

Best Practices for ePB Access: Both physical and cyber security are enhanced when an organization has well defined policies on who has access to the system. This includes both physical access, and access to the systems and equipment. You must control and actively monitor access. The Belfer Center Report [5] includes several best practices for access control.

- Limit the number of people with access to the [ePB] system to those who need it to complete their jobs (the "who"). [5] p.16
- Restrict what each user is authorized to do. [5] p.16
- Quickly remove those who no longer need access. [5] p.16

- Keep a list of all users who have access and their access levels.
- Regularly adjust access and permissions as personnel change. [5] p.19

Best Practices for ePB Operation:

- Make them single-purpose devices. [5] p.19 In other words, ePBs should not be used for any other purpose whether the ePB operates from a laptop or a tablet.
- Software on them should only be what is necessary. [5] p.19
- Understand how voter information is loaded onto the electronic poll books; confirm the electronic poll book file on the device matches the original file (Use hash codes if available). [5] p.19
- Ensure that the entire setup is preconfigured and that turning on devices is the only action required by election site workers (they should not need to change any settings on the devices).
- Ensure physical security. [5] p. 30
- Cover exposed ports (for example, USB) to prevent them from being accessed by anyone intending to inject malware via a USB or other portable device. [5] p.30
- Do not use anything other than the original charging cord [5] p.30 (for example, do not use an iPhone charger or other similar charger that is not actually part of the ePB)
- Discuss with your vendor if your county needs the electronic poll book to be connected to your vendor's resources (like a server). If you do not need the [electronic poll book] to be connected to a vendor, SVRS, or the Internet while voting is taking place: turn off Bluetooth and wireless capabilities on the devices. It is better to disable these functions at the hardware level (for example, removing the wireless card) than to change a setting whenever possible. [5] p. 30
- Have a paper backup of the electronic poll book at each voting location. Alternatively, the county election board can print paper poll books on demand on election day to distribute to voting locations should a data breach or other connectivity issue occur.

4. **Elections Cybersecurity Best Practices**

- The Belfer Center, Harvard Kennedy School has published *The State and Local Election Cybersecurity Playbook* (See Section 7). This report includes several recommendations for establishing or improving cybersecurity for elections. The recommendations include:
    - Monitoring, logging, and backing up data. This enables attack detection and system or data recovery after an incident.
    - Backups should be regularly performed, either through automation or as part of a scheduled manual process.
    - Backups should be read-only once created to prevent data corruption.
    - Backups should be regularly tested by performing a complete restore from backed-up data.
- The National Institute of Standards and Technology (NIST) has published the *Framework for Improving Critical Infrastructure Cybersecurity 1.0* [4]. This report contains several recommendations for establishing or improving a cybersecurity program, which may also apply to cybersecurity for elections. Steps for improving such a program include:
    - Prioritize and Scope: Identify your high-level organizational priorities based on the most current cybersecurity threats to elections and election technology (VSTOP can assist counties in this area).

    - Orient: Identify related systems and assets.
    - Conduct a Risk Assessment (please see *Cybersecurity 1.0* above or consult with VSTOP).
    - Determine, Analyze, and Prioritize Gaps (based on the difference between current practices and Best Practices and anything identified in a risk assessment)
    - Implement Action Plan (VSTOP can assist with this. Additionally, a county election official in the CEATS program can develop such a plan as a capstone project).
- Be aware of recent changes in the State statutes (such as Indiana Senate Enrolled Act 327 - 2018) that relate to cybersecurity of voting equipment. See Section 6.
- The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends
    - Securing networks and systems
        - Credential (e.g., usernames and passwords for logins) reuse policies
        - Use Two Factor Authentication (, a method whereby a user is required to enter more than a password, such as a code, to login to the system
    - Securing the End User (an "End User" is the ultimate consumer of hardware and software and in the instance of this manual would, in most cases, be an election official or poll worker)
    - Responding to a Compromise or Attack (Create a plan to respond to a compromise or attack on your election systems (ePBs or voting systems)
        - Detach the infected systems from the Network
        - Inform incident response team (IT Team) about attack
        - Run Anti-Virus and Anti-Malware on all systems to determine if other systems were infected
        - Delete all the infected files and restore the systems from the last backup before Infection.
    - Spear Phishing Tests (for an awareness of these attempts). Please see the glossary in this document for a definition of these types of campaigns.
- *The State and Local Election Cybersecurity Playbook* (See Section 7) also discusses Malware and its potential threat to voting equipment. One should treat all removable media as a potential delivery mechanism for malware. Some examples of Malware include the following.
    - Viruses – a type of malicious malware program that replicates itself, can corrupt and modify computer files, and can infect other systems
    - Trojan Horses – a malicious software program which entices a user to install it because it appears normal, routine or valuable for a system
    - Keyloggers – a covert method of computer keystroke recording whereby a malicious actor can log the keys used by a user to obtain valuable information such as usernames, passwords and other confidential information
    - Adware – a form of software that allows advertisements into a computer system and generates unwanted ads which may be of interest to a user
    - Spyware – a computer program which operates undetected in the background of a computer system in order to control a system or obtain information about the system and user without the user's knowledge
    - Worms – like viruses, worms can replicate themselves on a computer system using failures and limitations of the system's security in order to limit the system's capabilities
- If you need to connect an electronic poll book to external systems, there are certain security practices which should be followed. These include the following from *The State and Local Election Cybersecurity Playbook*:

  - Connect over a VPN (Virtual Private Network) or other encrypted channel. A VPN is a secure method of connectivity. [5] p.30
  - Ensure that the entire setup is preconfigured and that turning on devices is the only action required by election site workers (they should not need to change any settings on the devices). [5] p.30
  - Do not connect [electronic poll books] directly to the SVRS. Set up a separate system (essentially a copy of the SVRS) to handle changes to voter information, which prevents the SVRS from being impacted if an electronic poll book is compromised. [5] p.30
- The National Conference of State Legislators (NCSL) released the report *The Price of Democracy: Splitting the Bill for Elections* the day before on February 14, 2018 [6] which also includes suggestions and best practices for election security and cybersecurity. We also recommended a comprehensive review of this report. However, a few best practices pertaining to ePBs and VRDBs are noted here:
  - **Invest in cybersecurity personnel**. Hiring cybersecurity consultants or more IT staff may be useful. It can be helpful to work with outside experts, since they may be better prepared to find security holes than internal staff.
  - **Coordinate with others.** Sharing information within the state, between states, with federal agencies, and even between private entities can be the difference between discovering security holes and not. The Department of Homeland Security (DHS) offers cybersecurity assistance to election officials (see https://www.dhs.gov/topic/election-security), and there are organizations that help share security information between states as well, such as the Multi-State Information Sharing & Analysis Center (MS-ISAC). Some states have established partnerships with the National Guard to assist with protecting election systems from cyber threats. Private companies such as Google have also made commitments to providing assistance to state and local election officials (see: https://protectyourelection.withgoogle.com/intl/en/).
  - **Training.** Beefing up security can be as simple as providing training to state and local election officials on things like requiring strong passwords, activating existing security software that may be built into their systems, updating software as the vendor suggests, and teaching staff to avoid phishing and spear phishing efforts (please see the Glossary in this document for definitions of phishing and spear phishing). Overall, we must create a culture of security within election administration.
  - **Resiliency**. It's important for state and local officials to be able to monitor their systems, detect threats, respond, and then recover. What happens if the voter registration database is changed? Are there backups? Do state laws permit a "fail-safe" option for those who attempted to register but were thwarted by a cyberattack?
  - **Choosing secure equipment.** Security and resiliency of the systems can be a top-of-the-list priority. What is the backup in case of an attack on these systems?

5. **Elections Physical Security Best Practices**
   - In a presentation at the 2018 Election Administrator's Conference, Beth Dlug, Director of Elections, Allen County, Jay Phelps, Clerk, Bartholomew County, and Laura Herzog, Elections Supervisor, Hendricks County described many excellent best practices for physical security. Below are some examples. See a copy of the presentation for the entire list.
     - Ensure that your voting system complies with VVSG.
     - Review VSTOP's certification and audit standards (Please see the EAC and SOS/IED websites or contact VSTOP).

  - Seal voting systems after public tests, which is required under IC 3-11-13-26 (optical scan systems) and IC 3-11-14.5-7 (DRE).
  - Deliver voting systems to the polling location no later than 6:00 pm the day before election, which is required under IC 3-11-13-6 and 3-11-14-14.
  - Record seal numbers, provide documentation of seal numbers in election materials for poll workers to compare against.
  - If numbers do not reconcile or seals are broken, inform county election officials immediately.
  - Secure the equipment after polls close.
  - Secure Absentee ballots under bipartisan lock-and-key until election day.
- Be aware of recent changes in state election code (such as Indiana Public Law 100 - 2018) that relate to physical security of voting equipment. See Section 6.
- Maintain an inventory of the voting systems and electronic poll books as required by IC 3-11-16-5 and provide this information to VSTOP. See Section 6.
- The report *Election Security: A Priority for Everyone*, published in NCSL's The Canvass, July 2017 [7] includes the following best practices:
  - Ballot reconciliation. Accounting for all ballots, those that were voted, spoiled in some way and set aside, or never voted.
  - Chain of custody. "Chain of custody" requirements come into play when there are any movements or actions relating to ballots, poll books, equipment and just about anything else. It's common practice to log everything, and to require bipartisan teams to work together in this process.
  - Secure physical storage. Between one election and the next, elections equipment has to be kept somewhere. Is that warehouse secured? Is there a log of who enters and exits? Are security cameras used? Are unmarked ballots secured too? While legislation on storage requirements is rare, it's a key issue with local or state officials. See the U.S. Election Assistance Commission's paper on 10 Things to Know About Managing Aging Voting Systems for more information as well as Indiana's Public Law 100 - 2018 for physical security provisions.
  - Contingency planning. Planning for crises and disasters. For instance, how would your county address a data breach to an ePollbook or loss of internet connectivity? What is your plan if a polling location cannot be used on Election Day due to an emergency? What happens if a power line is cut to a polling place on Election Day - can your voting systems work on battery back-up or do you have paper ballots that can be securely stored until power is restored? Are your poll workers trained?

6. Standards and Best Practices based on the Indiana Election Code

This section includes a description of recent Indiana election law that relates to the physical security and cybersecurity of elections and election equipment. Be aware of changes in state election code that relate to physical security of voting equipment. The following became effective March 15, 2018 or July 1, 2018 in some cases, pursuant to Public Law 100 - 2018. In future versions of this manual, additional Indiana Code will be referenced. It should be noted that election officials should be aware of already existing security provisions in the Indiana Election Code in addition to recent changes.

Indiana Code	Best Practice
IC 3-6-3.7-5: This permits a county election board to apply to the Secretary of State for reimbursement of expenditures made by the county to secure and monitor facilities where voting systems and electronic poll books are stored.	Keep track of the inventory/locations and expenses.
IC 3-11-7-20, IC 3-11-7.5-24, IC 3-11-8-10.3 (c): The county election board is responsible for the security of ballot card voting systems, direct record electronic voting systems, and electronic poll books when they are not in use.	Utilize the VSTOP-ESI database for tracking the inventory and locations. Please see communication from VSTOP regarding the web location for the database.
IC 3-11-13-22, IC 3-11-14.5-1: The public tests should include tests for correct counting of straight party votes and write-in votes.	Revise your tests to include this requirement, as needed. Ask VSTOP for IED approved tests for straight party counting.
IC 3-11-15-46: The county election board is responsible for access policies and security protocols. The VSTOP and IED shall be available to advise the county election board in the development of a security protocol under this subsection.	Discuss with VSTOP and IED to develop such protocols. Please refer to the sample packet provided to county clerks at the June 2018 SBoA conference in Indianapolis.
IC 3-11-15-59: The county election board must have a plan for disposal of election equipment.	Utilize the VSTOP-ESI database for tracking the inventory. Please see communication from VSTOP regarding the web location for the database. Inform VSTOP and IED when there are items ready for disposal and utilize the state form for IED approval of disposal.
IC 3-11-16-4, IC 3-11-16-5: VSTOP must maintain an inventory of voting systems and electronic poll books. Each county election board shall regularly provide information to the program to update the inventory of voting systems and electronic poll books	Use VSTOP-ESI training materials to maintain a current inventory of your election equipment. Please see communication from VSTOP regarding the web location for the database and the user manual in that location.
IC 3-11-17-7: The county election board must report improper access to election equipment or data.	Maintain proper chain-of-custody records. This can be maintained, for example, in spreadsheet form by a county official. The spreadsheet would need to include the date, the person accessing equipment, the equipment being accessed by serial or inventory number, the time the person entered the equipment room, the time the person exited the equipment room, and any other notes.

7. **Resources**
   - **Federal and Other**
     - Election Assistance Commission and various versions of the Voluntary Voting System Guidelines (VVSG)
     - Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology (NIST), February 12, 2014
     - U.S. Department of Homeland Security
     - Election Center
     - NIST – Framework for Improving Critical Infrastructure Cybersecurity 1.0, National Institute of Standards and Technology
     - Voting System and Electronic Poll Books Vendor documentation
     - NCSL.org National Council of State Legislatures - ELECTION SECURITY: STATE POLICIES
     - The State and Local Election Cybersecurity Playbook, Defending Digital Democracy Project, Belfer Center, Harvard Kennedy School
     - Election Cyber Incident Communications Plan Template for State and Local Officials, Belfer Center, Harvard Kennedy School
     - Hacking Chads - The Motivations, Threats, and Effects of Electoral Insecurity, Belfer Center, Harvard Kennedy School
   - **State Level**
     - Indiana Department of Homeland Security - Election and Polling Place Emergency Preparedness Guide, October 22, 2012
     - Title 3 - Indiana Election Code
     - Indiana Election Division
     - Physical Security of Election Systems and Materials (Presentation by Beth Dlug et al. at the 2018 Election Administrator's Conference)

8. Glossary

The following Glossary of Information Technology and Election Administration terms is available at the U. S. Election Assistance Commission (EAC) website at https://www.eac.gov/documents/2017/09/21/information-technology-terminology-security/

General Information Technology

Access Controls Methods by which access to specific data, procedures, and other resources is restricted or controlled. The most common access control is a username/password combination. Two factor authentication (TFA) is highly recommended along with strong passwords made up of letters, numbers, and symbols.

Election officials must control access to resources within the scope of the election systems they supervise. A typical criteria is "need to know," implying that election workers only have access to appropriate data and resources within the scope of their responsibility.

Accessibility Refers to the extent to which a site, facility, work environment, service, or program is easy to approach, enter, operate, participate in, and/or use safely and with dignity by a person with a disability.

Election officials must ensure that all aspects of the election are fully accessible to all voters.

Accountability Methods by which a system associates users and processes.

Election officials must be able to detect when an error occurs by logging the event. A main function of event logging is being able to determine who is accountable for the error.

Administrative Controls The policies and procedures implemented as part of its overall information security strategy.

Election officials must create an IT and security strategy that addresses the policies and procedures for securing their election systems.

Air Gap An air gap is a physical separation between systems that requires data to be moved by some external, manual procedure. Also called "Sneaker Net."

Election systems often use air gaps intentionally to prevent or control access to a system. Copying election results to a CD or USB drive, then walking that media to a different computer for upload and use in a different system is an example of an air gap.

Algorithm A procedure or formula that produces predictable, consistent results when applied. An algorithm describes, in formal language (frequently mathematical) how a problem is solved. An algorithm, like a recipe, is a well prescribed sequence of steps designed to produce a solution.

The procedure that produces a uniform distribution of ordered candidates within a race in a ballot rotation scheme is an algorithm. Counting votes in an instant runoff voting system requires a specific algorithm.

Application Programming Interface (API) Specification for input data and output data for a system.

Election officials can use APIs to adapt their election systems for commonly used applications, such as the Voter Information Project (VIP) for voter lookup tools and election night reporting

Assistive Technology A device that improves or maintains the capabilities of people with disabilities (no vision, low vision, mobility, cognitive, etc.).
Assistive technologies include headsets, keypads, software, sip-and-puff, and voice synthesizers.

Accessibility of voting systems in accomplished through good, universal design principles and assistive technologies.

Audit A review of a system and its controls to determine its operational status and the accuracy of its outputs.

Election system audits seek to determine if controls are properly designed and functioning to ensure the correctness of intermediate and final results of the system's processing.

Audit trail The records that document transactions and other events. Some audit trails in election systems are event logs, paper records, error messages, and reports.

Authentication The process of identifying a user, usually by means of a username and password combination. Election systems use authentication methods to assure that only those users with appropriate authority are permitted access to the system. Authentication schemes should not permit group logins.

Backdoor An undocumented or hidden entry into a computer system that permits unauthorized access to programs and/or data. Some early voting systems had backdoors that permitted developers to access system functionality without logins.

Bandwidth The throughput capacity of digital connections. Large data files (like an electors list) require significant bandwidth capacity to move through a network. Low bandwidth means slow connection speeds.

Barcode A barcode is an optical, machine-readable representation of data relating to an object. Barcodes come in a variety of formats including 1D (barcode 39 or 128) and 2D (pdf 417). Barcodes can also be encrypted. Barcoding is a common technique to permit rapid identification of ballots, election materials, and voter records.

Blacklist A list of URLs, domains, users, or other identifiers, that have system access or privileges blocked. Election offices may wish to "add" domains to be blocked to a blacklist, maintained by their system administrator.

Blockchain A database that holds a continuously growing set of encrypted transactions, in a tamper proof format. Blockchain is the underlying architecture for Bitcoin technology. Online voting systems have been proposed that use Blockchain architecture.

Boolean Pertaining to one of two states: off/on, 1/0, Yes/No, or some other binary pairing. When a voting system is tested, most of the tests are Boolean in nature – that is, the system completely passes or completely fails the test.

Botnet A programmed Internet connected device that can be used to launch DDOS attacks, steal data, send spam, etc. Bots are frequently spread as email attachments and can compromise election office computers used to browse websites and support email activities.

Browser Software program installed on a computer, that permits the user to access the Internet, download files, print files, and perform other operations. Common browsers are Microsoft's Internet Explorer, Mozilla's Firefox, and Apple's Safari. Not all applications will run on every browser. Election Night Reporting Systems, voter information pages, and other Internet applications may appear different, in different browsers. Check systems for browser compatibility.

Byte Eight binary digits or the amount of data used to store a character or an integer – a measurement of storage in a computer's memory or its storage media. The average voter record consists of about 200 characters. That would require 200 bytes of storage, plus some storage for meta data. To store 6 million voter records on a memory card, that card needs to have at least 1.2 Giga Bytes of memory.

Ciphertext Data or information in its encrypted form. Election data will display in cyphertext – and be unreadable by humans – without decryption.

Cloud Computing The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Also called on-line computing.

Election technologies are evolving in parallel with other commercial information systems. Election officials may be managing voter and election data, stored on computers, outside of their organization. Cloud computing requires an appropriate security strategy to ensure the protection, availability and integrity of data and programs store in the cloud.

Code n. Synonym for program or software. v. to create or modify software.

Commercial Off-The-Shelf Technology (COTS) Hardware and software components that are widely available for purchase and can be integrated into special-purpose systems.

E-pollbooks are often implemented on COTS tablets such as the iPad or Android tablet. COTS systems are contrasted with propriety systems.

Common Data Format Standard and practice of storing and creating data in a common, described format that can be read by other systems.

Voting and election systems that use a common data format can share data without middleware software to convert it. Election Night Reporting systems are common applications that anticipate a common data format for input.

Controls A device, procedure, or subsystem, which when properly designed and implemented, ensures correctness of operation in a system. Common controls include completeness of processing checks, authentication of users, and accuracy in processing. Controls can be preventative (prevent anomalies from occurring) or paired, detective and corrective controls.

A common detective control in election administration is a physical seal. The seal does not prevent tampering with election devices but permits the detection of tampering.

Custodian Person with the responsibility for protecting information assets.

IT personnel or an IT Division may be the custodian of voter registration systems and other systems that are maintained in house. For a precinct-based voting system, the custodian may be an election worker who is in charge verifying seals and making sure no unauthorized access is gained to the voting devices.

Cybersecurity Measures taken to protect computer systems from attack and unauthorized access or use. Cybersecurity tools include hardware, software and procedures.

Election officials must defend against attacks and unauthorized access of election and voting systems. The most common cybersecurity technique is good password management.

Data destruction The removal of data from a storage medium.

Election officials should destruct all data on election systems before selling or disposing of the systems. Any election system that is to be destroyed should use a reputable company and best practices for destruction, so that data cannot be obtained after it is no longer in the custody of the election official.

Database A structured collection of data that includes data and meta data (data about the data). Databases are managed by Database Management Systems.

The election database stores all of the requisite information to manage election including precinct

information, race and candidate information, and data used to prepare the ballots, tabulate, and report results.

Defense-in-Depth Also called the "Castle" approach. Multiple levels of logical and physical security measures that deny a single point of security failure in a system.

The use of passwords, encryption, lock-and-key access, security seals, and logs, represents a defense-in-depth approach to securing voting and election systems.

Digital Certificate A technology by which systems and their users can employ the security applications of Public Key Infrastructure (PKI). PKI is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Voting and election systems will use PKI infrastructure to exchange and compare digital certificates for the purpose of authenticating access and securing transmission of data.

Digitize To convert analog data to digital format for storage and use on a computer. The digital form of the character "A" is the byte: 01000001 (ASCII value 65). Any data stored in a computer must be digitized. Converting the information on the front of a voter ID card or driver's license into a computer readable format requires the data to be digitized. Scanners are digitizers.

Directory A file storage architecture in which individual files are stored in separate, hierarchical directories. The directory is the map to where the file is stored. Most systems will store files in a default directory unless otherwise specified.

Election systems will store files in directories on both internal and external storage media. Finding a file requires the election official to know not only the file name, but also the directory name in which the file is stored.

Domain A collection of users, computers, and resources that have a common security policy administered by a single entity.

Download Transferring data from a larger computer to a smaller computer or device.

An EMS facilitates downloading ballot images to vote capture devices.

Dox Publish damaging or defamatory information about an individual or organization on the Internet.

One method of hacking a campaign is doxing (or doxxing).

Dynamic password A password that changes at a defined interval or event.

Entitlement Access rights assigned to employees based on job title, department, or other established criteria.

Ethernet A network protocol (IEEE 802.n) that is used to permit local area network devices to communicate with each other. Ethernet connections use a Cat 5e connector cable.

Many of the devices used in polling places will use an Ethernet connection to establish connectivity with other devices (e-pollbooks, card activators, etc.).

Encryption The process of encoding messages or information in such a way that only authorized parties (or software applications) can read it.
Encryption does not prevent interception but denies the message content to the interceptor. Encrypted information must be decrypted before it can be rendered into plain text or other usable format. Encryption and decryption add overhead to processing and can slow systems down.

Voting systems will commonly encrypt data within a voting system component before transmitting it to another device.

End of Life (EOL) When the manufacturer or integrator of an IT component ceases to produce and provide technical support for that product.

Election officials who use technologies that are EOL'd, should monitor available inventories and begin to create a transition strategy to newer, supportable technology.

Escalation of privilege An attack where the attacker is using some means to bypass security controls in order to attain a higher privilege level on the target system.

Exfiltration – Unauthorized transfer of information from an information system.

A data breach of an election system may lead to the exfiltration of PII data.

Failover A mode where the system automatically transfers processing to a backup component when a hardware or software failure is detected.

Fail-safe A mode where program execution is terminated to protect the system from being compromised when a hardware or software failure is detected.

Fail-soft A mode where non-critical processing is terminated to protect the system from being compromised when a hardware or software failure is detected.

Failure The inability of a system or component to perform its required functions within specified performance requirements.

Fault Momentary loss of electrical power.

Fault-Tolerant A system that continues to operate after the failure of a computer or network component.

File A collection of related data, stored on media. Files will be identified by a system-valid filename.

File type – The specific kind of information contained in a file, usually designated with a file extension (for example, .doc for a Word document; .txt for a text document, etc.). A .pdf file is common format for reports (See **Portable Document Format)**

Systems will usually expect a specific file type for input/output operations. Your election night reporting system may accept only a .txt file or a .zip file.

FIPS (Federal Information Processing Standards) Standards issued by US Government for use in government agencies. FIPS 140 covers encryption standards.

Firewall A gateway computer and its software that protects a network by filtering the traffic that passes through it.

Election offices often need to reconfigure the firewall to permit large files or complex files to be passed through the firewall that separates the office from the internet.

Firmware Computer instructions that are encoded directly into computer hardware. Firmware is resident to the hardware and cannot be altered without modifying the hardware.

Voting systems may contain firmware that cannot be altered without replacing the hardware.

FTP (File Transfer Protocol) A standard network protocol used to transfer computer files between a client and server on a computer network, usually the Internet.

Election offices will upload and download files, such as sample ballots or election databases, using an

FTP site. FTP requires the use of password authentication.

Gateway A system, connected to a network, which performs real-time translation or interface function.

Glitch An intermittent system error of undetermined cause. A system glitch may cause a network to go offline or a program to crash.

Election officials are expected to track down all errors to their root causes and avoid blaming anomalies on "glitches."

Hacker Someone who seeks to exploit weaknesses in computer systems, voting systems or networks to gain unauthorized access or break-in into a system. There are many types of hackers, but the best-defined terms for types of hackers are white-hat and black-hat hackers

Hacking The act performed by a hacker whereby the hacker gains unauthorized access or breaks-in into a system by exploiting a weakness.

Hacktivism Utilizing technology to publicize a social, ideological, religious or political message.

Hacktivism can refer to any attempt to alter or influence the outcome of an election by an interested third party, such as a nation state. It can also refer making information that is not public, or is public in non-machine-readable formats, accessible to the public

Hardware The physical, tangible, mechanical or electromechanical components of a system. If you can put an inventory sticker on it – it's hardware.

Voting system hardware must be physically secured with locks, seals, and logs. Hardware may be COTS or proprietary. Proprietary hardware is unique to the vendor and purchase, maintenance and repairs will be done by the voting system vendor. Hardware can be repurposed by upgrading the software that controls it.

Hash Function A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes

Voting system object code is "hashed" so that installations can be validated as identical to the certified version.

Heterogeneous environment An environment consisting of multiple types of systems.

Homogeneous environment An environment consisting of a single type of system.

Hub A network device used to connect several LAN devices together.

Hypertext Transfer Protocol (HTTP) An application protocol to transfer data between web servers and web browsers.

Hypertext Transfer Protocol Secure (HTTPS) The HTTP protocol encrypted with SSL or TLS.

Inactivity timeout A mechanism that locks, suspends, or logs off a user after a specified period of inactivity.

Interface A boundary between two components of a system**,** through which the components may interacts or share information.

Examples: A hardware interface connects input/output devices. Humans and computers interact though user interfaces.

A DRE presents an interface to the voter. This interface permits the voter to interact with the system via a touchscreen, wheel, or some other input device.

Internet Global, public network that permits computers and other devices to be interconnected.

Election offices may have desktop, laptops, tables and other computers connected to the Internet so that information can be uploaded and downloaded and applications like email can be run. Once a device is connected to the Internet it is potentially accessible by anyone, from anywhere. Internet access carries with it certain security risks.

Internet Service Provider (ISP) Organization that provides access to the Internet for customers or members.

Examples include AT&T, Comcast, etc.

Interoperability The extent to which systems and devices can communicate with each other and work cooperatively without extensive modification by a systems integrator or programmer.

The extent to which you can change out components of a system is a measure of the interoperability of that system. Generally speaking, interoperability permits an election official a wider range of options for maintenance and support of their voting system.

Intranet A local network of computers and other devices that moves and stores information within the organization.

Election offices may use an intranet to store election related data that is not accessible from outside of the office.

Intrusion detection system (IDS) A hardware or software application that detects and reports a suspected security breach, policy violation or other compromise that may adversely affect the network.

Intrusion prevention system (IPS) A hardware or software application that detects and blocks a suspected security breach, policy violation or other compromise that may adversely affect the network.

IP Address Internet Protocol Address. An IP Address is numeric value (nnn.nnn.nn.nn) used to uniquely identify a device within a network. The address can also be used for local networks.

Many devices in an election office may be linked together on a local network that utilized IP addressed to identify devices. Accurate settings of the IP address are critical to permit devices to communicate with each other.

Java applet A software application written in the Java programming language that is usually launched through a web page. Browsers must be configured to interpret Java applets.

ENRs and Voter Information Pages often include Java applets.

Local Area Network (LAN). Also see MAN and WAN. A computer network that connects computer and other devices such as printers in a limited area such as a school, office building or home.

Computers and devices in an Election Management Center may be connected with a LAN.

Life Cycle Systems engineering concept that identifies the phases that a system passes through, from concept to retirement. There are different concerns and activities associated with each phase of the life cycle.

The adoption, deployment, use and maintenance of voting and election systems require different life cycle concerns and activities, depending upon where in the life cycle the system resides.

Malware Various types of malicious software intentionally designed to cause damage to a computer, server or computer network.

Message digest A condensed representation of a message that is produced by using a one-way hash function.

Multi-factor authentication Authentication mechanism requiring two or more of the following: something you know (for example, Password), something you have (for example, Token), something you are (for example, biometrics).

National Institute of Standards and Technology (NIST) Federal organization tasked with assisting in the development of voting system standards (see VVSG). NIST develops and maintains standards for a wide array of technologies.

NIST scientists assist the EAC in developing testable standards for voting systems.

Open Source Computer software with its source code (human readable code) made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose. Open source software may be developed in a collaborative public manner.

Voting and election systems that contain open source software have had that software reviewed by multiple, professional and amateur programmers.
Open source systems are usually not free and are typically licensed like other software. Systems can be fully open source, or may have only a portion of their software open source.

Operating System A collection of programs that controls the hardware of a computer system and provides utilities and services to application software that is installed on the device. Operating systems use complex release version numbers to indicate which version is installed and require frequent patches or updates to maintain security and functionality.

Managing the software revisions in an election office requires careful coordination of updates to the operating system as well as to the application software.

Owner An individual responsible for management of an asset and its policies.

Penetration Testing Also called Pen Testing. An evaluation method that enables researcher to search for vulnerabilities in a system.

Election systems, such as the VR system, are periodically submitted to Pen Test to determine their vulnerabilities to cyber-attacks.

Phishing A general attack by hackers, via bogus emails, that attempts to get victims to provide login information or personal information to the hackers. Phishing attempts may appear to originate from legitimate, known sources, such as organizational IT or known vendors.

Election officials should NOT click through on suspicious links or open attachments without first verifying that the email is legitimate.

PII Personal Identifying Information. Information that permits the identity of an individual to be derived and possibly used for identity theft.
Voter registration systems may contain PII.

Portable Document Format (pdf) A standard and commonly used file format, used for creating, sharing, and reading documents, forms, and reports. Pdf files can only be opened and read by a reader, such as Adobe Acrobat.

A lab report for a voting system and a form for voter registrations are common examples of pdf files.

Preventive controls Controls that prevent unwanted events.

Program *n.* A set of instructions that are stored within a computer's memory and cause the computer to execute a task. *v.* The process of creating a computer program.

Election databases are programmed to store all the data as well as the rules of processing that data, for a given election. Ballot builders are sometimes referred to as election database programmers.

Protocol 1. An agreed upon format for transmitting data between devices. 2. A plan for carrying out a formal or scientific study.

Voting system tests are often called protocols.

Proxy server A system that transfers data packets from one network to another.

QR Code Quick Response Code. A 2-D, trademarked bar code.

Some proprietary voting systems will encode the voter's choices in a QR Code that can be read on a scanner in the precinct and converted to a printed ballot.

Ransomware Malware that holds the victim's device (computer, phone, etc.) and data for ransom, by means of encrypting the files on the device or preventing access to the device.

Election office computers should maintain high levels of cyber hygiene, including up-to-date anti-malware systems and adherence to best practices regarding managing browser and email client activities.

Requirements The fundamental collection of activities and functions that must be supported by a system. Defining requirements determines the capabilities of the system.

Election officials must be able to articulate the fundamental set of things a voting system or election system must do, in order to define the requirements of the system. These requirements are then reiterated in Request for Proposals (RFPs) and subsequent contracts with vendors.

Router A device that manages network traffic by passing data packets between different networks.

A wireless router may be used to permit EPBs to communicate with each other at a precinct or vote center.

Server A server is a collection of computer programs, hosted on a computer that provides services to other computers, via some connection – usually a network.

Voting systems use special-purpose servers to create closed networks for uploading and downloading information from voting system media (memory cards). These servers also contain the tabulation software.

Social Engineering Misleading users into providing information that can be used to compromise the security of a system. Usually low-tech.

Social engineering of election officials includes emails and phone calls requesting information that can be used to spoof accounts or hack passwords.

Software A synonym for program. Computer software is the collection of programs that control the computer and perform a specific collection of tasks. Software has version numbers and is licensed (not sold) to the end user. Software can be altered to change the functionality of the computer.

The Election Management System (EMS) used to create election databases is software.

Source Code Human readable computer instructions that when compiled or interpreted, become an application. Source code can be written by humans or by computers. The source code of a voting system must be securely stored (escrowed) so that any future, needed modifications of the system can be performed.

Spear Phishing A targeted attack by hackers (toward a particular person or entity), via bogus emails, that attempts to get the victim to provide login information or personal information to the hackers. Spear Phishing attempts may appear to originate from legitimate, known sources, such as organizational IT or known vendors.

Election officials should NOT click through on suspicious links or open attachments without first verifying that the email is legitimate.

Switch Switches connects computers in a network. A switch acts as a controller. Thus, switches create networks. Routers connect and manage traffic between different networks.

One or more DREs might be connected via a switch to the EMS.

System A collection of unified components that convert inputs to outputs. Systems consist of integrated subsystems. Systems are typically complex and highly interconnected. Information systems consist of hardware, software, data, people and procedures.

The voting system is more than just a single device. It consists of numerous subsystems, which when unified and controlled, give the voting system its capabilities. Subsystems include vote capture, vote tabulation, reporting, etc.

Software Patches Also called fixes or bug fixes. Corrections to existing programs, designed to be integrated into the programs without major release changes.

Patches or fixes to voting systems must be tested before being applied, and may invalidate certifications. Do not install software patches without extensive technical review for unintended consequence.

Tabletop Exercise A discussion-based drill where qualified personnel discuss scenarios and responses in order to validate plans and procedures. Also called Incident Response Planning.

Election officials exchange in tabletop exercises to determine the viability of their election continuity plans.

Uninterruptable Power Supply (UPS) A battery powered back-up system that quickly switches to battery power when electrical current to the computer system is disrupted (surge, sags, and failures). Election offices ensure election operations continuity by utilizing UPS systems in the event of a power failure. UPS systems come in various sizes and are rated by hours/minutes of service following a power failure.

Upload Transfer data from a smaller computer or device to a larger computer.

At the close of polls, memory cards with cast ballot information are uploaded to the central tabulation computer.

Virtual Provide Network (VPN) A VPN is a secure method of computer system connectivity.

Virus A malicious computer program that may replicate itself on in a computer network, insert or attach copies of itself into computer programs, and cause harm to computers or systems by corrupting, stealing or modifying data or access.

Voting system components connected to a network risk malware infections, such as viruses.

Wi-Fi Wi-Fi is a wireless networking technology that uses radio waves to provide wireless high- speed Internet and network connections. Wi-Fi is a trademarked phrase for the *IEEE 802.11x* standard. Wireless is less secure than Ethernet connections.

Some e-pollbook and voting system technologies use Wi-Fi or wireless connectivity at the polling place.

Wide Area Network (WAN) A network that connects computers across metropolitan, regional and national boundaries.

The internet is an example of a WAN.

Wireless Network connectivity using radio waves instead of wire connections. Wireless signals can be intercepted and, if not encrypted, deciphered.

Election systems that use wireless connectivity must be tested for security and signal reliability.

XML Extensible Markup Language XML is a text-based language used to organize and present information on the World Wide Web. Some Election Night Reporting (ENR) systems use XML coding for their displays. The voting system must be able to export reports in (or convert them to) XML format.

Election Administration Technology

Acceptance Testing Testing each individual unit of the voting system for conformance to the certified model. Acceptance testing should not be done by the vendor and should be done any time the voting system unit falls out of custody of the jurisdiction. In Indiana electronic poll books also undergo acceptance testing.

Automatic Voter Registration (AVR) Voter registration subsystem that creates a voter record automatically from an external (usually DMV) transaction. AVR systems require a voter to "opt out" if they choose not to be registered (It should be noted that Indiana does not have automatic voter registration. However, Indiana does have "motor voter").

Ballot On Demand (BOD) Ballot On Demand systems permit a jurisdiction to print paper, optical scan ballots as needed. BOD systems integrate ballot images from the EMS and data from the voter registration system to select the correct image for printing. In theory BOD systems prevent over ordering of ballots and ensure that the jurisdiction does not run out of ballots during the election.

Barcode Reader Device used to scan barcodes and convert the encoded information into a usable format. Barcode readers are used to scan codes on ballots, driver's licenses, voter ID cards, voter information packets, envelopes, and other documents in the election ecosphere.

Central Count Optical Scan Optical scan system that utilizes one or more high-speed scanners at a central location to tabulate ballots. Central count systems are usually paired with Vote By Mail technologies.

Digital Optical Scan System Optical scan system that converts voter choices on a paper ballot to digital values. Digital op scan systems can accommodate a broader range of paper types, sizes of paper, ballot layout, and voter marks than IR op scan systems. Often these systems have an electronic interface for a voter to mark their candidate selections digitally and an optical scan paper ballot card is printed with their selections. The ballot card is then inserted into the optical scan component of the system where the results are tabulated.

Direct Record Electronic Voting System (DRE) A DRE system presents a ballot image to a voter, collects the voter's choices, and records those choices directly onto electronic media. DREs may be fitted

with Voter-verifiable paper audit trail (VVPAT) subsystems to create a paper artifact of the voting transaction. DREs are capable of audio interaction, image displays, and can hold a large number of ballot styles in multiple languages.

Election Management System (EMS) The collection of software systems that are used by election officials to "build ballots." The EMS defines ballots by associating precincts with races and candidates and describing how those ballot components will be displayed. The EMS is also responsible for tabulation, report generation and auditing.

Election Night Reporting Systems (ENR) A web-based system that aggregates and displays unofficial election results across the jurisdiction. ENR systems can be real-time or near real-time, and acquire their data from the EMS. ENR systems can provide multiple formats for displaying election results and may provide direct feeds for the media.

Electronic Ballot Delivery The delivery of ballot and voter information packets via the Internet. The Military & Overseas Voter Empowerment Act (MOVE) requires each state to provide for the electronic delivery of ballots and related information from the local election office to the registered voter covered by the Uniformed & Overseas Citizens Absentee Voting Act (UOCAVA).

Electronic Ballot Return The return of a voted ballot or voter information packet via electronic means. This can be by fax, email, or through the use of an Internet supported application. Sometimes referred to as "Internet Voting."

Electronic Poll Book (EPB) Hardware and/or software that permits election officials to review the list of registered voters and mark voters who have been issued a ballot. Also called e-pollbook. E-pollbooks can be stand alone at the precinct with a separate copy of the electors list, or can be networked into a central voter registration system and check and update voter records in real time.

Geographical Information System (GIS) A system designed to capture, store, manipulate, analyze, manage, and present all types of spatial or geographical data. GIS systems are used to validate voting district boundaries and may be integrated with the voter registration system.

High Speed Central Count Tabulation System An optical scanner capable of scanning a high number of ballots (hundreds) per minute. These large and complex scanners are typically used in vote-by- mail jurisdictions, in large jurisdictions that have a large number of absentee ballots, or in central count jurisdictions.

Logic and Accuracy (L&A) Testing Several jurisdictions around the United States are required to test the correctness of every ballot style and to determine that every possible valid and invalid voter choice can be captured or handled by the voting system, both technologically and legally. L&A scripts are developed to test both the ballot and the vote capture and tabulation systems.

Indiana Jurisdictions are not required to do L&A testing; instead, they are required to conduct a public test. Before the public test of voting systems, county election administrators are strongly encouraged to perform L&A testing. This is a pre-test of the voting system using an audited deck of ballots with a pre-determined outcome to ensure all candidates receive a vote, and in a November election the straight party option is also tested. Further, the test deck must test for an over-vote for counties using an optical scan system and an under-vote in counties using an optical scan system or DRE. L&A testing ensures any issues with system coding can be corrected before the legally required public test of voting systems.

Online Voter Registration (OVR) Voter registration subsystem that permits individual users to remotely create, edit or review their own voter record within the voter registration system.

However, in Indiana voters do not create or edit their record within the system. A person may submit an

application to register to vote or update an existing registration, though the changes are not automatic and require county validation and the mailing of a voter acknowledgment card.

Optical Scan System (Op Scan) A voting system that can scan paper ballots and tally votes. Most older op scan systems use Infrared (IR) scanning technology and ballots with timing marks to accurately scan the ballot.

Precinct Count Optical Scan Optical scan technology that permits voters to mark their ballot cards within a precinct and submit the ballot for tabulation. Precinct Count systems provide overvote/undervote protection.

Remote Ballot Marking Devices Remote ballot marking systems are used in some jurisdictions nationwide, which assist military and overseas voters in completing their ballot. These allow a voter to obtain an official ballot which is blank that can then be marked electronically, printed, and returned to an elections office as a ballot to be cast in an election.

Risk Limiting Audit Risk-limiting audits provide statistical assurance that election outcomes are correct by manually examining portions of paper ballots or voter-verifiable paper records.

Technical Data Package (TDP) A collection of documents that describe a voting system, including manuals, a description of components and details of architectural and engineering design.

Voluntary Voting System Guidelines (VVSG) Collection of standards that is developed and maintained by the U.S. Election Assistance Commission (EAC). The VVSG specifies a minimum set of performance requirements that voting systems must demonstrate when tested by the VSTLs. Please see https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/

Vote By Mail (VBM) Method of casting ballots by which eligible voters are mailed ballots and information packets by the local jurisdiction. Voters can return their marked ballots by mail or drop them off in secure drop boxes. Vote By Mail replaces Election Day voting at polling locations, and should not be confused with Indiana's absentee-by-mail option.

Voter Registration System (VRS) A distributed or centralized system that permits the collection, storage, editing, deletion and reporting of voter records. HAVA requires each state to have a centralized, statewide voter registration system (VRS). A VRS has multiple interfaces and can interact with Department of Motor Vehicle (DMV) systems, election officials, voters and other stakeholders. The VRS may be vendor-provided or "homegrown."

Voting System The total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information.

Voting System Test Labs (VSTLs) VSTLs are privately owned testing laboratories that test voting systems (and other election systems) for conformance to the Voluntary Voting System Guidelines (VVSG) or to other requirements, including individual state requirements. VSTLs are periodically reviewed for conformance to National Voluntary Laboratory Accreditation Program (NVLAP) administered by the National Institute for Standards and Technology (NIST). In 2016, there were three accredited VSTLs.

Voter Verified Paper Audit Trail (VVPAT) Contemporaneous (or real-time) paper-based printout of voter choices on a DRE.

End Notes

1. Ten Things to Know About Selecting a Voting System, Managing Election Technology Series #1, United States Election Assistance Commission https://www.eac.gov/assets/1/28/Managing%20Election%20Technology%20Series%201%20Ten%20Things%20FINAL.6.24.15.pdf
2. "Indiana Electronic Poll Book (ePollBook) Certification Test Protocol," http://www.in.gov/sos/elections/files/doc00354920170908122519.pdf
3. 10 Things to Know About Managing Aging Voting Systems, *Managing Election Technology Series #2,* https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-managing-aging-voting-systems-voting-technology-voting-systems-cybersecurity/
4. Framework for Improving Critical Infrastructure Cybersecurity 1.0, National Institute of Standards and Technology, https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf
5. The State and Local Election Cybersecurity Playbook by Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#securing
6. The Price of Democracy: Splitting the Bill for Elections by the National Conference of State Legislators (NCSL), http://www.ncsl.org/research/elections-and-campaigns/the-price-of-democracy-splitting-the-bill-for-elections.aspx
7. Election Security: A priority for everyone by the National Conference of State Legislators (NCSL), http://www.ncsl.org/research/elections-and-campaigns/states-and-election-reform-the-canvass-july-2017.aspx#Election%20Security

Voting System Technical Oversight Program at Ball State University (VSTOP)

Risk Limiting Audit (RLA) Pilot

May 2018

Post-Election Risk Limiting Audit Pilot

Marion County Indiana

May 30, 2018

An Introduction

A Collaboration between Marion County Office of the Clerk, Office of the Indiana Secretary of State, Indiana Governor's Executive Council on Cybersecurity, U.S. Election Assistance Commission, Caltech/MIT Voting Technology Project, and the Voting System Technical Oversight Program (VSTOP)

VSTOP

Indianapolis

U.S. ELECTION ASSISTANCE COMMISSION

Secretary of State

Caltech/MIT
Voting Technology Project

Introduction

In January 2017, U.S. Elections Systems were designated as part of the nation's critical infrastructure by the United States Department of Homeland Security. Also, in January 2017, Indiana Governor Holcomb signed an Executive Order to continue the Indiana Executive Council on Cybersecurity (IECC) (https://www.in.gov/cybersecurity/2570.htm). The Executive Council comprises ten committees and several working groups. The Elections Committee of the Council is chaired by the Indiana Secretary of State Hon. Connie Lawson. Dr. Jay Bagga of the Voting System Technical Oversight Program (VSTOP) serves as an Advisory Member to this Council and is a member of the Elections Committee.

One of the deliverables for the Elections Committee is to create a **Post-election risk limiting audit (RLA)** protocol proposal. As a component of this activity, VSTOP proposed conducting a pilot RLA in some Indiana counties. VSTOP began discussing the RLA process with Jerome Lovato, Election Technology Specialist at the U. S. Election Assistance Commission.

VSTOP considered several counties for such an audit. It is important to note that only jurisdictions with Voter Verifiable Paper Ballots are amenable to RLAs. VSTOP selected Marion County for this and a variety of other reasons, including its high voter registration. With the approval of Secretary Lawson and the Co-Directors of the Indiana Election Division, VSTOP held discussions with Marion County Elections Officials to discuss a potential partnership. VSTOP was pleased that in April 2018 Marion County agreed to be our partner for this endeavor.

The RLA Pilot will be conducted in Marion County, Indianapolis on May 30, 2018. In planning for this audit, Mr. Lovato proposed that the RLA Pilot include methods proposed by Dr. Philip B. Stark (Berkeley) and Dr. Ronald L. Rivest (MIT). These methods, the RLA method and the Bayesian Method will be used in the pilot for several races from the 2016 and 2018 elections. The races we are planning to audit are the Presidential Race from the November 2016 General Election, the U.S. Senate Race from the November 2018 Republican Primary Election, and the Sheriff Race from the 2018 Democratic Primary Election.

Marion County uses the ES&S EVS 5.2.2.0 which is an OpScan Voting System. This voting system is used in five other Indiana counties. The experience gained from a successful pilot audit can serve as the basis for RLA replication in other counties.

The RLA Pilot Team has relied on many of the lessons learned from the State of Colorado which was the first state to mandate Risk Limiting Audits as part of their post-election audit procedures. At this time not all Counties in Indiana have the capability to conduct a Post-Election Audit because we are not aware of any Direct Recording Electronic (DRE) Voting machines certified in the state of Indiana that produce a voter-verifiable paper audit trail.

VSTOP, Mr. Lovato, Dr. Rivest, as well as members of Marion County Elections Officials have held weekly WebEx planning meetings since the beginning of May. The RLA Pilot Team will meet at the Marion County Election Service Center on the afternoon of May 29th to organize and prepare for the Audits to be held on May 30th.

Based on a process assessment and the outcome of this initial Post-Election Audit initiative, VSTOP will advise the Indiana Secretary of State and the Governor's Indiana Executive Council on Cybersecurity regarding the future potential uses of post-election audits within the state of Indiana.

A Brief Overview of Risk Limiting Audits

Risk limiting audits (RLAs) provide statistical assurance that election outcomes are correct by manually examining paper ballots or voter-verifiable paper records. RLAs do not guarantee that the electoral outcome is right, but they have a large chance of correcting the outcome if it is wrong. If the original outcome is wrong, there is a chance the audit will not correct it. Thus, the risk limit is the largest chance that an incorrect outcome escapes correction. For instance, if the risk limit is 10% and the outcome is wrong, there is at most a 10% chance (and typically much less) that the audit will not correct the outcome—at least a 90% chance (and typically much more) that the audit will correct the outcome. Thus, if the risk limit is 1%, then, in the long run at least 99 out of 100 wrong outcomes would be corrected by the audit.

The number of ballots required to conduct an RLA will vary based on the smallest margin of the contest selected and the risk limit. The smaller the margin, the more ballots to audit. The smaller the risk limit, the more ballots to audit.

Computer software cannot be guaranteed to be perfect or secure, so voting systems should be software-independent – An undetected change or error in voting system software should be incapable of causing an undetectable change or error in an election outcome. An RLA leverages software independence by checking the audit trail strategically. Efficient RLAs do not require complicated calculations or in-house statistical expertise.

An RLA software program is used to calculate the number of ballots to audit, randomly select the ballots, provide a ballot lookup table, and notify the user when the audit can stop. The audits depend on sampling methodology as well as statistical methodology. There are four types of sampling methodologies: ballot polling, ballot comparison, batch polling, and batch comparison. Additionally there are two types of statistical methods: RLA and Bayesian.

In 2009, Colorado's HB 09-1335 introduced RLAs to commence with the 2014 General Election. In 2013, Colorado conducted the first pilot RLA at Arapahoe County. More counties were added in 2015-16. Colorado developed rules, procedures, and software to conduct an RLA for the 2017 Coordinated Election. The November odd-year election is generally referred to as the coordinated election. Coordinated elections are conducted by mail ballot.

In 2014, Cuyahoga County, Ohio, conducted a risk limiting audit for its gubernatorial race. Incumbent John Kasich received 51 percent of the votes cast in the county, and challenger Edward FitzGerald received 45 percent. The county Board of Elections needed to recount slightly more than 8,000 ballots before it could confidently determine that Governor Kasich had correctly been declared the winner. The board also audited the race for state treasurer, in which incumbent Joshua Mandel received 39 percent of the vote versus 61 percent for challenger Connie Pillich. In this less competitive contest, fewer than 2,500 ballots were needed to certify Pillich's victory among county voters.

The California secretary of state recently completed a three-year pilot program that audited contests of varying size in counties throughout the state.

In September 2017, Rhode Island became the second state to require risk limiting audits, for implementation by 2020, with possible pilots in 2018.

References

- A Gentle Introduction to Risk-limiting Audits, by Mark Lindeman and Philip B. Stark, IEEE SECURITY AND PRIVACY, SPECIAL ISSUE ON ELECTRONIC VOTING, 2012. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf
- A Bayesian Method for Auditing Elections https://www.usenix.org/system/files/conference/evtwote12/rivest_bayes_rev_073112.pdf

For more details please see the PowerPoint presentation by Jerome Lovato at the end of this document. This PowerPoint may differ slightly from the final presentation provided on May 30th.

Marion County Post-Election Audit Pilot Agenda

Location: Election Service Center at 3737 E. Washington St., Indianapolis, IN 46201

Day 1 – May 29th 12:00 PM – 4:30PM

12:00 PM	VSTOP: Introductions
12:15 PM	County: Review state/county guidelines for handling ballots and accessing restricted areas
12:30 PM	County: Walk through procedure for organizing and storing ballots
1:00 PM	J. Lovato: Provide Risk Limiting Audit (RLA) overview to county officials (Q&A)
1:30 PM	Create/Review Ballot Manifests, organize ballots for audits
3:00 PM	Ensure Primary ballots are separated by Democratic and Republican categories, nonpartisan, if applicable
4:00 PM	Phone Conference with Secretary Lawson

Day 2 – May 30th 8:30 AM – 3:30 PM

8:30 AM	VSTOP: Introductions J. Lovato: Risk Limiting Audit overview Dr. Rivest: Bayesian Audit Method
9:15 AM	Ballot Polling Audit of 2016 Presidential Race in Precincts LA-02, WS-49, PE-39, WR-23 and WS-69
10:00 AM	Break
10:15 AM	Ballot Polling Audit of 2018 Republican U.S. Senate Race in Precincts TBD
11:00 AM	Ballot Polling Audit of 2018 Democrat Marion County Sheriff in Precincts TBD
Noon	Remarks by Secretary Connie Lawson
12:15 PM	Lunch Break
1:30 PM	Bayesian Audit of 2016 Presidential, 2018 Primary R-U.S. Senate Race 2018 Primary D-Sheriff Race
2:15 PM	J. Lovato: Example/demo of comparison audit procedures
3:00 PM	Conclusion

The RLA Pilot Team

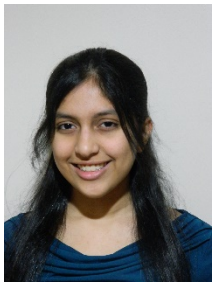
Jerome Lovato, Election Technology Specialist, U. S. Election Assistance Commission (EAC)

Jerome received his Bachelor of Science in Electrical Engineering from the University of Colorado at Denver. After working as an electrical engineer in the consumer electronics industry for six years, he worked as a Voting Systems Specialist at the Colorado Secretary of State's office for 10 years as a Voting System Certification Lead and Risk-Limiting Audit Project manager. Currently, he is an Election Technology Specialist for the U.S. Election Assistance Commission. Jerome led the team in Colorado that employed the RLA method. The following link is a gentle introduction to this method: https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

Dr. Ronald L. Rivest, Institute Professor at MIT

Professor Rivest is an Institute Professor at MIT. He joined MIT in 1974 as a faculty member in the Department of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and a founder of its Cryptography and Information Security Group. He is a co-author (with Cormen, Leiserson, and Stein) of the text, *Introduction to Algorithms*. He is also a founder of RSA Data Security, now named RSA Security (the security division of EMC), Versign, and Peppercoin. Professor Rivest has research interests in cryptography, computer and network security, electronic voting, and algorithms. A paper on the Bayesian method can be found at: https://www.usenix.org/system/files/conference/evtwote12/rivest_bayes_rev_073112.pdf

Mayuri Sridhar, Research and Innovation Scholar, MIT



Mayuri Sridhar is a Master's student studying Artificial Intelligence at MIT. She completed her undergraduate degree at MIT, double majoring in computer science and mathematics. Her research, under Profesor Rivest's supervision, focuses on statistics and optimization, applied to election audits.

Marion County Clerk's Office

Myla A. Eldridge, County Clerk
Brienne Delaney, Director of Elections
Jenny Troutman, Deputy Director of Elections
Joanna Alexander, Absentee Administrator
Colin Claycomb, Ballot Administrator
Rhonda Hawkins, Service Center Manager
and other county staff personnel

The VSTOP Team

Dr. Jay Bagga and Dr. Bryan Byers, VSTOP Co-Directors
Jessica Martin, VSTOP Project Manager
Mani Kilaru, VSTOP IT Specialist
Molly Owens, VSTOP Graduate Assistant
Contact: VSTOP@bsu.edu

Statistical Post-Election Audit Pilot at Marion County, IN

Jerome Lovato, Election Technology Specialist
U.S. Election Assistance Commission

Goals

We will conduct a ballot-polling risk-limiting audit (RLA) and Bayesian audit. If time allows, we will also a conduct a comparison RLA.

The data gathered from this pilot will be used by the Voting System Technical Oversight Program (VSTOP) to assist in their development of a post-election audit protocol proposal for Indiana, and will be used by other jurisdictions throughout the U.S. that are considering conducting post-election audits using these methods.

Statistical Audit Methods - Terminology

A risk-limiting audit provides strong statistical evidence that the election outcome is right, and has a high probability of correcting a wrong outcome.[1] There are two main types of RLAs: ballot-polling and comparison.

The risk limit is the largest chance that a wrong outcome will not be corrected. If the risk limit is 5% and the outcome is wrong, there is at most a 5% chance that the audit will not correct the outcome, and at least a 95% chance that the audit will correct the outcome.

A Bayesian audit is a statistical tabulation audit that provides assurance that the reported contest outcome is correct, or else finds out the correct contest outcome.[2]

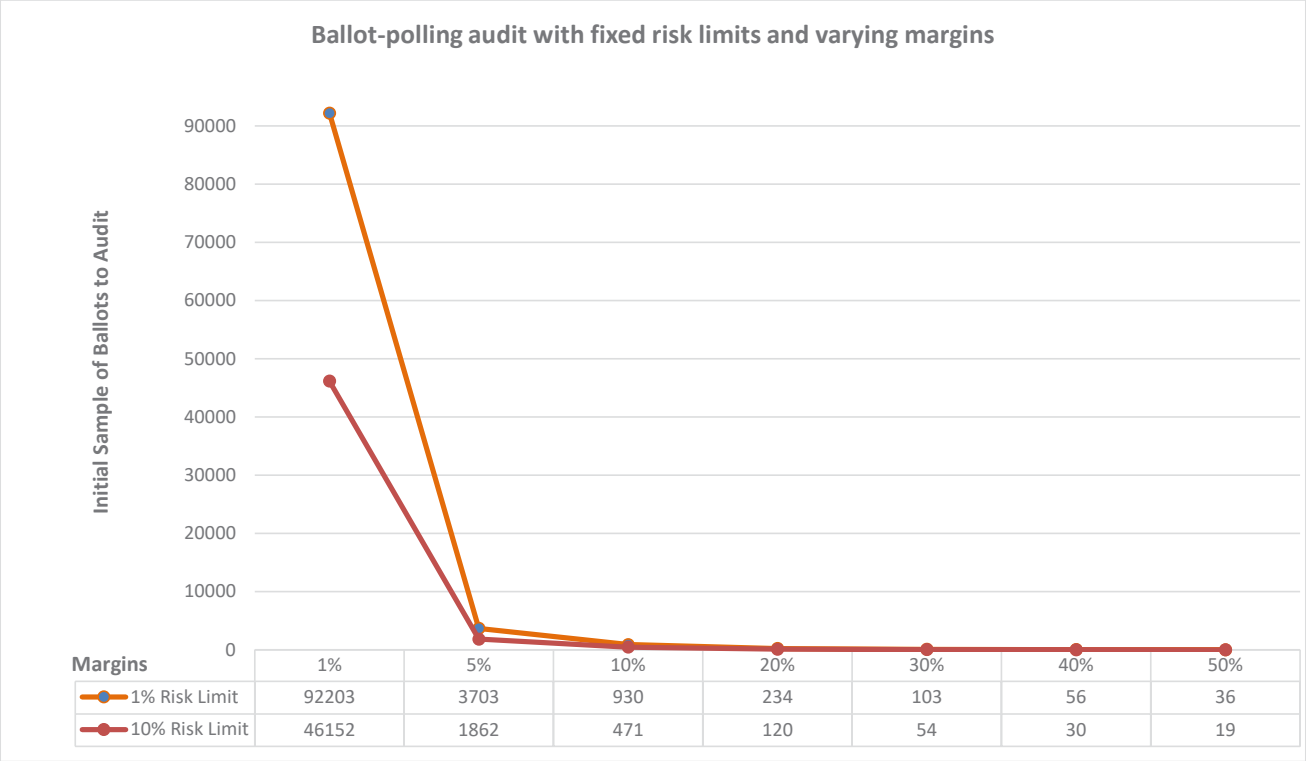
A Bayesian risk limit is a desired upper bound on the probability that the audit will make an error (by accepting an incorrect reported contest outcome as correct).

About Ballot-Polling RLAs

A ballot-polling RLA is similar to an exit poll. In this case, ballots (people) are randomly selected and tabulated (polled).

Pros	Cons
Minimal set-up costs	May require additional human resources
Does not require information from the voting system	Does not provide information about errors
Efficient for margins of 10% or greater	Inefficient for margins less than 10%

Ballot-Polling RLAs by the Numbers



Margins	1%	5%	10%	20%	30%	40%	50%
1% Risk Limit	92203	3703	930	234	103	56	36
10% Risk Limit	46152	1862	471	120	54	30	19

About Bayesian Audits

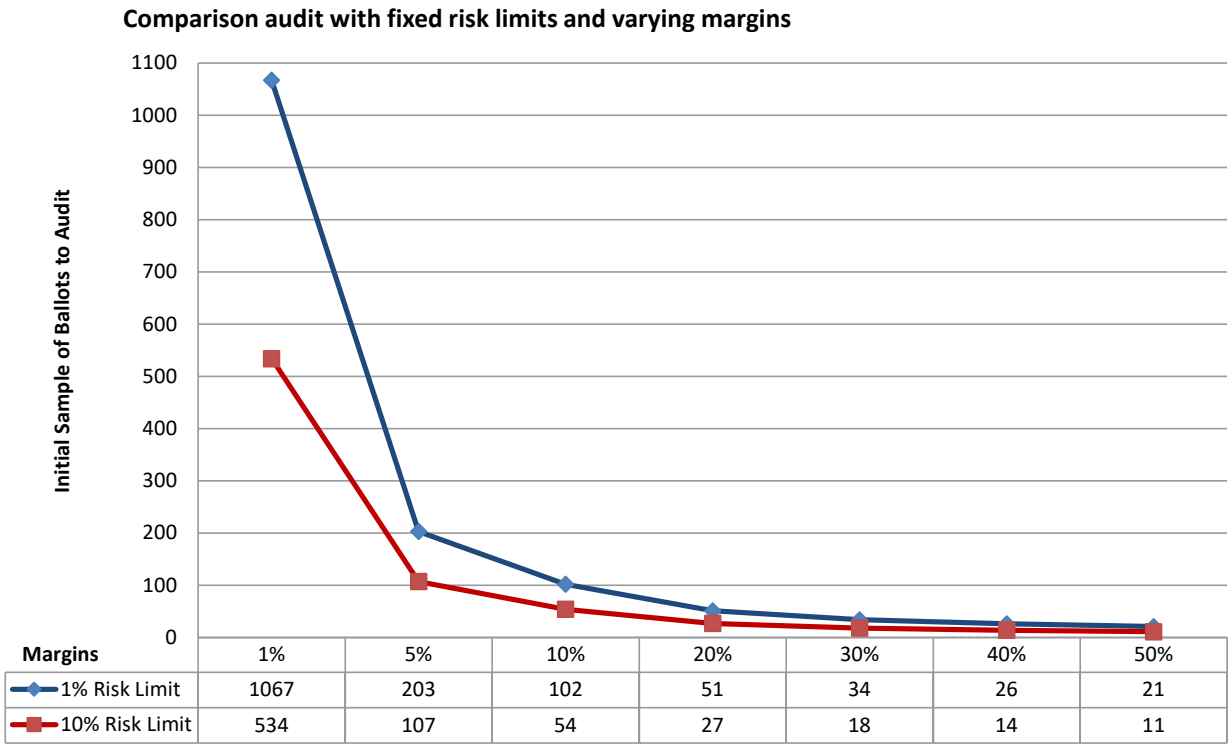
Pros	Cons
Automatically provides a measure of risk at each point	It is simulation-based and software dependent
Does not require information from the voting system	Costs are unknown
Efficient for cross-jurisdictional contests and other voting methods	Requires a level of trust from the public since the computations are not transparent

About Comparison RLAs

In a comparison RLA, individual ballots are randomly selected and compared to the CVR for each ballot.

Pros	Cons
Requires fewer human resources to conduct an audit	Depends on a voting system that can produce a CVR
Allows the auditor to correct any errors	Retrieving specific ballots can be difficult and time consuming
Efficient for margins of any size	Requires maintaining ballots in the exact order they are scanned, or imprinting numbers on the ballots

Comparison RLAs by the Numbers



Margins	1%	5%	10%	20%	30%	40%	50%
1% Risk Limit	1067	203	102	51	34	26	21
10% Risk Limit	534	107	54	27	18	14	11

Uniform Audit Procedures

The uniform procedures that apply to the audit methods used are:

1. Maintain documented chain-of-custody for all ballots cast.
2. Create a ballot manifest, which is a document that describes how ballots are organized and stored.
3. Determine the risk limit.
4. Determine what contest(s) will be audited.
5. Decide what other utilities (software, calculator, spreadsheets, etc.) will be used to calculate the number of ballots to audit, randomly select the ballots, provide a ballot lookup table, and notify the auditor when the audit can stop.
6. Obtain a cast vote record (CVR) from the voting system (this is only used for comparison RLAs). A CVR is an export of data from the voting system showing how the voting system interpreted markings on every ballot.

Marion County Pilot Procedures

Ballot-Polling RLA

Using Dr. Stark's ballot-polling RLA tool[3] and the ballot manifest, we will obtain our initial sample of ballots to audit for each of the selected contests. The Marion County election staff will select the ballots, tabulate the results of each ballots, and the result will be entered into the audit tool. If the risk limit is not met with the initial sample of ballots, we will continue to select ballots until it is met.

Bayesian Audit

We will enter the sample of ballots obtained from the ballot-polling RLA into Dr. Rivest's Bayesian audit tool[4] which will compute the estimated probability of winning a full manual recount. Given a Bayesian risk limit of 5%, the Bayesian audit will stop when the auditor is at least 95% certain that the reported contest outcome is correct.

Comparison RLA

We will use Dr. Stark's comparison RLA tool[5] and the ballot manifest to obtain our initial sample of ballots to audit. The Marion County election staff will compare the selected ballots to their CVRs. If there are no discrepancies, the audit will stop after the initial sample has been audited. If discrepancies are discovered, we may have to audit additional ballots (depending on the type of discrepancy).

Marion County Pilot Parameters

Risk Limit = 10%

Bayesian Limit = [***?***]

Contests to audit:

- 2016 Presidential
    - Estimated sample size (ballot-polling RLA) = ?
    - Estimated sample size (comparison RLA) = ?
- 2018 Republican U.S. Senate
    - Estimated sample size = [?]
    - Estimated sample size (comparison RLA) = ?
- 2018 Democrat Marion County Sheriff
    - Estimated sample size = [?]
    - Estimated sample size (comparison RLA) = ?

Sample Ballot Manifest

Precinct ID	Total # of Ballots	Precinct Batch ID	# of Precinct Ballots	Absentee Batch ID	# of Absentee Ballots
LA-03	400	LA-03P	300	LA-03A	100
WS-49	400	WS-49P	300	WS-49A	100
PE-39	600	PE-39P	400	PE-39A	200
WR-23	600	WR-23P	400	WR-23A	200
WS-69	600	WS-69P	400	WS-69A	200

What is Now

IC 3-11-13-38

Petition for confirmation of vote cast

Each county chairman for either of the major parties in the county may petition the county election board for confirmation of the vote cast on a ballot card voting system no earlier than the Saturday before an election and no later than the Thursday after an election. The petition may specify not more than five percent (5%)of the precincts or five (5) precincts, whichever is greater, in which a ballot card voting system was used for an audit under section 37 of this chapter.

What is Next

- Conduct additional pilots at counties of different sizes that use different voting systems.
- Determine what entity will serve as the central audit authority.
- Determine what method(s) will best serve Indiana.
- Draft laws and procedures for conducting an audit.
- Train local election officials on how to conduct audits.

- **Implement a statistics-based post-election audit.**

Notes

1. The ballot-polling and comparison RLAs were developed by Dr. Philip Stark, Associate Dean, Division of Mathematical and Physical Sciences at University of California - Berkeley, and Dr. Mark Lindeman, Adjunct Assistant Professor of Political Science at Columbia University. These methods have been tested by various jurisdictions around the U.S., and were implemented by Colorado beginning with the November 2017 election. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

2. Dr. Ron Rivest, Vannevar Bush Professor of Electrical Engineering and Computer Science at MIT, developed the Bayesian audit method that will be tested for the first time in Marion County, Indiana. https://arxiv.org/pdf/1801.00528.pdf

3. Ballot-Polling RLA Tool: https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm#

4. Bayesian Audit Tool: http://audits.csail.mit.edu/

5. Comparison RLA Tool: https://www.stat.berkeley.edu/~stark/Vote/auditTools.htm#

Contact

Jerome Lovato
jlovato@eac.gov
(202)805-4163

Social media

Email
listen@eac.gov

Facebook
Facebook.com/eacgov1

Twitter
@EACgov

Youtube Channel
Election Assistance Commission

Website
www.eac.gov

Voting System Technical Oversight Program at Ball State University (VSTOP)

Risk Limiting Audit (RLA) Pilot Report

August 2018

Risk Limiting Audit (RLA) Pilot
Marion County, Indiana
on
May 29-30, 2018

A Report to
the Indiana Secretary of State
August 15, 2018

By

Voting System Technical Oversight Program
(VSTOP)
Ball State University

Introduction and Background

Much has been reported in the news media in the last few years about the integrity of American elections and the security of voting equipment. This national discussion has centered on two key areas. First, the physical and cyber security of election equipment, and, second, the public's confidence in election equipment, the process of elections, and election outcomes. It is noteworthy that the Indiana Secretary of State Connie Lawson has been at the forefront of this discussion, both at the national and state levels, and has acted to address real and perceived threats to elections. There are several recent key events and items which are relevant to the present report. These include Indiana Governor's Executive Council on Cybersecurity, the Hoosier Survey, a recent report by the Center for American Progress, and the new Indiana election law addressing election security.

According to the website[1], "Signed by Governor Holcomb on Jan. 9, 2017, the Indiana Executive Council on Cybersecurity (Council) was continued through Executive Order 17-11 with the recognition that a cross-sector body of subject-matter experts is required to form an understanding of Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment. Led by the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana State Police, and the Indiana National Guard, the Council is made up of government (local, state, and federal), private-sector, military, research, and academic stakeholders to collaboratively move "Indiana's cybersecurity to the Next Level." With 35 Council members and almost 250 advisory members, the Council will deliver a comprehensive strategy plan to Governor Holcomb by September 2018." One of the standing committees of the Council is for Elections which is chaired by Secretary Lawson.

In September of 2017, The Bowen Center for Public Affairs included survey questions on the 2017 Hoosier Survey regarding *perceived* voter confidence and problems with elections. The survey, which covered a wide variety of topics, was administered to a representative sample of 600 Indiana residents. The Hoosier Survey was conducted by Princeton Survey Research Associates International for Ball State University. The two questions germane to the present report and the responses appear in Tables 1 and 2 below.

Table 1
What level of confidence do you have that your vote in the last election was properly recorded and accurately counted?

Confidence Level	Percentage
Very confident	60%
Somewhat confident	23%
Not too confident	8%
Not confident at all	9%
Don't know/refused to answer	<1%

While 60% of the respondents felt "very confident" that their vote in the last election was properly recorded and accurately counted, nearly 40% of respondents were "somewhat," "not too" or "not at all" confident regarding their vote. This finding speaks to the power of perception regarding the integrity of elections. While elections are marked by general high levels of integrity, public perception is something which must be addressed along with physical and cyber protections for elections.

[1] https://www.in.gov/cybersecurity/2570.htm

Table 2 presents data on a related question and addressed perceived problems with elections. In response to this question, 53% of the respondents reported that the biggest problem with elections was "voter fraud" with 31% reporting it to be "denying eligible voters the right to vote."

Table 2
Thinking about elections in the United States, which of the following do you believe is a bigger problem?

Problem Area	Percentage
Voter fraud	53%
Denying eligible voters the right to vote	31%
Both equally	7%
Neither	4%
Don't know/refused to answer	4%

Perceptions, whether or not grounded in reality, are important to consider when addressing elections and election integrity. Thus, one part of the equation in addressing election integrity is the physical and cyber security needed to protect elections while the other is addressing the public perceptions which exist around elections. In addition to issues raised through public perceptions, there are also special interest organizations which have examined elections and election security. One of these is the Center for American Progress (CAP).

On February 15, 2018 the Voting System Technical Oversight Program (VSTOP) received a communication from General Counsel Jerry Bonnet in the Office of the Indiana Secretary of State. Mr. Bonnet sent VSTOP a copy of the Center for American Progress (CAP) Report *Election Security in All 50 States - Defending America's Elections.* Mr. Bonnet asked VSTOP to review the CAP report and comment on the report and the methodology that led to Indiana receiving a "grade of F." VSTOP's response presented an assessment of the CAP report and the methodology employed by the authors to grade the 50 states on how the states were "faring in meeting even the minimum standards necessary to help secure their elections." The report awarded points based on the assessment of states' activities in seven categories: Cybersecurity standards for voter registration systems; Voter-verified paper audit trail; Post-election audits; Ballot accounting and reconciliation; Return of voted paper absentee ballots; Voting machine certification requirements; and Pre-election logic and accuracy testing. VSTOP's review found that the categories and the weights given to the categories seemed arbitrary, with no clear justification provided. Emerging activities such as post-election audits, which few states had implemented at the time of the report, were given three times the weight than other important and established election security areas such as voting machine certification requirements. States that used DREs in even a *single* jurisdiction were given an unsatisfactory rating in one of the categories, which seemed a harsh criticism of a practice currently followed by several states. Of greater concern, VSTOP's review indicated that the authors seemed unaware of Indiana's achievements in the seven categories. In some cases, the authors used outdated data, while in others even impressive data mentioned in the report was not reflected in the points or ratings awarded to Indiana. VSTOP concluded that the grade of "F" awarded to Indiana did not reflect a true and accurate picture of the many achievements in Elections Security and in the seven categories explored by the CAP authors. One of the areas in the CAP report given heavy emphasis was the use of Risk-Limiting Audits (RLAs) as a means of post-election audits of election outcomes. VSTOP and the Indiana Secretary of State were actively exploring the use of RLAs in the state when the report was being constructed and were also planning the first RLA pilot in the state.

On May 29 and 30, 2018, the VSTOP Team conducted Indiana's first RLA pilot in Marion County, Indiana. This pilot was carried out in collaboration with Mr. Jerome Lovato, Certification Program Specialist at the US Election Assistance Commission (EAC), Dr. Ronald L. Rivest, Institute Professor at MIT and a member of the Caltech/MIT Voting Technology Project, and Ms. Mayuri Sridhar, a Research and Innovation Scholar at MIT. Appendix A provides the handout for the RLA packet that was distributed to all parties. VSTOP could not have completed this work without the generous help and cooperation of Marion County Clerk Myla Eldridge and her elections staff, Ms. Brienne Delaney, Director of Elections & Ms. Jenny Troutman, Deputy Director of Elections. Indiana Secretary of State Connie Lawson, Chief of Staff and Deputy Secretary Brandon Clifton, their staff, Indiana Election Division Co-Directors Brad King and Angie Nussmeyer were all involved in the organization of this RLA Pilot. We appreciate the visit by the Secretary, Brandon Clifton, Brad King, Angie Nussmeyer, and Valerie Warycha (Deputy Chief of Staff and Director of Communications & Media Contact) at the audit site.

Risk Limiting Audits

Risk limiting audits (RLAs) provide statistical assurance that election outcomes are correct by manually examining paper ballots or voter-verifiable paper records. RLAs do not guarantee that the electoral outcome is right, but they have a large chance of correcting the outcome if it is wrong. If the original outcome is wrong, there is a chance the audit will not correct it. Thus, the risk limit is the largest chance that an incorrect outcome escapes correction. For instance, if the risk limit is 10% and the outcome is wrong, there is at most a 10% chance (and typically much less) that the audit will not correct the outcome—at least a 90% chance (and typically much more) that the audit will correct the outcome. Thus, if the risk limit is 1%, then, in the long run at least 99 out of 100 wrong outcomes would be corrected by the audit.

The number of ballots required to conduct an RLA will vary based on the smallest margin of the contest selected and the risk limit. The smaller the margin, the more ballots to audit. The smaller the risk limit, the more ballots to audit.

Computer software cannot be guaranteed to be perfect or secure, so voting systems should be software-independent – An undetected change or error in voting system software should be incapable of causing an undetectable change or error in an election outcome. An RLA leverages software independence by checking the audit trail strategically. Efficient RLAs do not require complicated calculations or in-house statistical expertise.

An RLA software program is used to calculate the number of ballots to audit, randomly select the ballots, provide a ballot lookup table, and notify the user when the audit can stop. The audits depend on sampling methodology as well as statistical methodology.

In 2009, Colorado's HB 09-1335 introduced RLAs to commence with the 2014 General Election. In 2013, Colorado conducted the first pilot RLA at Arapahoe County. More counties were added in 2015-16. Colorado developed rules, procedures, and software to conduct an RLA for the 2017 Coordinated Election. The November odd-year election is generally referred to as the coordinated election. Elections in Colorado are conducted by mail ballot.

In 2014, Cuyahoga County, Ohio, conducted a risk limiting audit for its gubernatorial race. Incumbent John Kasich received 51 percent of the votes cast in the county, and challenger Edward FitzGerald received 45 percent. The county Board of Elections needed to recount slightly more than 8,000 ballots before it could confidently determine that Governor Kasich had correctly been declared the winner. The

board also audited the race for state treasurer, in which incumbent Joshua Mandel received 39 percent of the vote versus 61 percent for challenger Connie Pillich. In this less competitive contest, fewer than 2,500 ballots were needed to certify Pillich's victory among county voters.

The California Secretary of State recently completed a three-year pilot program that audited contests of varying size in counties throughout the state. In September 2017, Rhode Island became the second state to require risk limiting audits, for implementation by 2020, with possible pilots in 2018.

While there is a large set of references on RLAs, the following two provide comprehensive introductions and details.

- A Gentle Introduction to Risk-limiting Audits, by Mark Lindeman and Philip B. Stark, IEEE SECURITY AND PRIVACY, SPECIAL ISSUE ON ELECTRONIC VOTING, 2012. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf
- A Bayesian Method for Auditing Elections https://www.usenix.org/system/files/conference/evtwote12/rivest_bayes_rev_073112.pdf

There are four types of sampling methodologies: ballot polling, ballot comparison, batch polling, and batch comparison. Additionally, there are two types of statistical methods: RLA and Bayesian. These are described below.

In the ballot polling sampling, one randomly draws ballots, examines ballots by hand and tallies results for each ballot. For ballot comparison, ballots are randomly drawn, examined by hand and each ballot is compared to its cast vote record (CVR). For batch polling, one randomly draws batches, examines results by hand, and tallies results for each batch. Finally, for batch comparison, one randomly draws batches, examines ballots by hand, tallies results for each batch and compares each batch to its batch report produced by the voting system. Ballot-level audits are more efficient than batch-level since they require examining fewer ballots. A comparison audit is more efficient but requires CVRs. Polling can be used if CVRs are not available.

The Stark RLA provides strong statistical evidence that the election outcome is right, and has a high probability of correcting a wrong outcome. The risk limit is the largest chance that a wrong outcome will not be corrected. If the risk limit is 5% and the outcome is wrong, there is at most a 5% chance that the audit will not correct the outcome, and at least a 95% chance that the audit will correct the outcome. The Stark audit tool can be found at the following link:
https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

A **Bayesian audit** is a statistical tabulation audit that provides assurance that the reported contest outcome is correct, or else determines the correct contest outcome. A **Bayesian risk limit** is a desired upper bound on the probability that the audit will make an error (by accepting an incorrectly reported contest outcome as correct). The Bayesian audit tool can be found at the following link:
https://arxiv.org/pdf/1801.00528.pdf

The Stark RLA is more popular and statistically rigorous. The Bayesian is more flexible and can be used in non-standard situations.

RLAs are valuable because these can detect problems with election outcomes, with a high degree of statistical confidence, without having to engage in an expensive and time-consuming full recount unless it is absolutely necessary. Further, the outcomes from RLAs can enhance voter confidence that votes were

correctly counted and tabulated. Moreover, RLAs serve as a check on the integrity of election outcomes based on statistical methods which confirm winners.

The Marion County, Indiana RLA Pilot

On the afternoon of May 29, 2018, VSTOP and the RLA team prepared for the RLA by obtaining ballots collected from selected precincts which would be used to draw samples of ballots for the "Ballot Polling RLA" as well as a cast vote record for a "Comparison RLA."

The RLA Team audited three races in the RLA pilot. These were:

- 2016 Presidential Election (5 precincts) – 2602 ballots cast (see Appendix B - Section 1 for full RLA details)
    - Needed to audit 61 ballots. Used Ballot Polling method to select this sample
    - Stark and Bayesian methods worked as expected and confirmed the "Clinton" outcome in the Marion County precincts with high levels of statistical assurance

- 2018 Primary Democratic Sheriff (10 Precincts) – 1747 ballots cast (see Appendix B - Section 2 for full RLA details)
    - Needed to audit 169 ballots. Used a combination of Three-Cut and Ballot Polling methods to select this sample
    - Stark and Bayesian methods worked as expected and likely would have confirmed the "Forestal" outcome with high levels of statistical assurance
    - However, these audits were ceased early due to time constraints

- 2018 Republican U.S. Senator (Comparison Polling Audit) – 1490 ballots cast (see Appendix B - Section 3 for full RLA details)
    - Due to time limitations, we elected to restrict the population size by randomly selecting 30 ballots using the Three-Cut method. This group of ballots was then treated as the population from which 16 ballots were selected for the sample using the Three-Cut method
    - Simulated CVRs were used for comparison
    - The audit ceased early but did not contradict the election outcome for "Braun" as the winner

The first RLA confirmed Clinton as the winner in the precincts audited for the 2016 general election for president. This was a fully completed RLA. The next two RLAs, although ceased early due to time constraints, did not contradict what would be expected in the selected precincts with Forestall the winner for the Democratic Sheriff's primary and Braun as the winner in the Republican U.S. Senate primary. As one examines the small number of ballots which needed to be sampled and examined for each of the three RLAs, one can appreciate the power of these methods as accurate predictors of election outcomes.

The experience was positive and valuable in learning how RLAs operate in the field. It is noteworthy that this was the first time that the Bayesian Audit Method was used in the field.

Jessica Martin, VSTOP Project Manager observed an RLA held in Denver County, Colorado July 5-6, 2018. Her reflections on this experience appear in Appendix C.

Conclusion

VSTOP is comfortable moving forward with additional pilot audits in the state at the Secretary's discretion. VSTOP believes at least one additional pilot is necessary since two of the races audited were ceased early due to time constraints. Nevertheless, there is no reason to believe the outcome would have been contradicted based on the actual winners given how well the audits were progressing given real-time results. VSTOP believes it would be a good practice to spend two full days to completely finish a future pilot audit in a different county with paper ballots in order to test the methods again and to gain additional experience with Risk-Limiting Audits. Additionally, there is value in completing RLAs on a variety of voting systems and vendors. With more experience in conducting RLAs, VSTOP will explore making recommendations to the Secretary regarding the feasibility and benefits of implementing RLAs statewide where applicable.

Acknowledgment

The VSTOP Team wishes to acknowledge and thank Secretary Lawson and her staff, Indiana Election Division, Jerome Lovato, Professor Ron Rivest, Mayuri Sridhar and the Marion County Clerk's Office staff (especially Brienne Delaney and Jenny Troutman) for their support and assistance with this project and report.

Appendix A

Post-Election Risk Limiting Audit Pilot

Marion County Indiana
May 30, 2018

An Introduction

A Collaboration between Marion County Office of the Clerk, Office of the Indiana Secretary of State, Indiana Governor's Executive Council on Cybersecurity, U.S. Election Assistance Commission, Caltech/MIT Voting Technology Project, and the Voting System Technical Oversight Program (VSTOP) at Ball State University

VSTOP

U.S. ELECTION ASSISTANCE COMMISSION

Indianapolis

Secretary of State

Caltech/MIT
Voting Technology Project

Introduction

In January 2017, U.S. Elections Systems were designated as part of the nation's critical infrastructure by the United States Department of Homeland Security. Also, in January 2017, Indiana Governor Holcomb signed an Executive Order to continue the Indiana Executive Council on Cybersecurity (IECC) (https://www.in.gov/cybersecurity/2570.htm). The Executive Council comprises ten committees and several working groups. The Elections Committee of the Council is chaired by the Indiana Secretary of State Hon. Connie Lawson. Dr. Jay Bagga, Co-Director of the Voting System Technical Oversight Program (VSTOP) serves as an Advisory Member to this Council and is a member of the Elections Committee.

One of the deliverables for the Elections Committee is to create a **Post-election risk limiting audit (RLA)** protocol proposal. As a component of this activity, VSTOP proposed conducting a pilot RLA in some Indiana counties. VSTOP began discussing the RLA process with Jerome Lovato, Election Technology Specialist at the U. S. Election Assistance Commission.

VSTOP considered several counties for such an audit. It is important to note that only jurisdictions with Voter Verifiable Paper Ballots are amenable to RLAs. VSTOP selected Marion County for this and a variety of other reasons, including its high voter registration. With the approval of Secretary Lawson and the Co-Directors of the Indiana Election Division, VSTOP held discussions with Marion County Elections Officials to discuss a potential partnership. VSTOP was pleased that in April 2018 Marion County agreed to be our partner for this endeavor.

The RLA Pilot will be conducted in Marion County, Indianapolis on May 30, 2018. In planning for this audit, Mr. Lovato proposed that the RLA Pilot include methods proposed by Dr. Philip B. Stark (Berkeley) and Dr. Ronald L. Rivest (MIT). These methods, the RLA method and the Bayesian Method will be used in the pilot for several races from the 2016 and 2018 elections. The races we are planning to audit are the Presidential Race from the November 2016 General Election, the U.S. Senate Race from the November 2018 Republican Primary Election, and the Sheriff Race from the 2018 Democratic Primary Election.

Marion County uses the ES&S EVS 5.2.2.0 which is an OpScan Voting System. This voting system is used in five other Indiana counties. The experience gained from a successful pilot audit can serve as the basis for RLA replication in other counties.

The RLA Pilot Team has relied on many of the lessons learned from the State of Colorado which was the first state to mandate Risk Limiting Audits as part of their post-election audit procedures. At this time not all Counties in Indiana have the capability to conduct a Post-Election Audit because we are not aware of any Direct Recording Electronic (DRE) Voting machines certified in the state of Indiana that produce a voter-verifiable paper audit trail.

The VSTOP Team, Mr. Lovato, Dr. Rivest, as well as members of Marion County Elections Officials have held weekly WebEx planning meetings since the beginning of May. The RLA Pilot Team will meet at the Marion County Election Service Center on the afternoon of May 29th to organize and prepare for the Audits to be held on May 30th.

Based on a process assessment and the outcome of this initial Post-Election Audit initiative, VSTOP will advise the Indiana Secretary of State and the Governor's Indiana Executive Council on Cybersecurity regarding the future potential uses of post-election audits within the state of Indiana.

A Brief Overview of Risk Limiting Audits

Risk limiting audits (RLAs) provide statistical assurance that election outcomes are correct by manually examining paper ballots or voter-verifiable paper records. RLAs do not guarantee that the electoral outcome is right, but they have a large chance of correcting the outcome if it is wrong. If the original outcome is wrong, there is a chance the audit will not correct it. Thus, the risk limit is the largest chance that an incorrect outcome escapes correction. For instance, if the risk limit is 10% and the outcome is wrong, there is at most a 10% chance (and typically much less) that the audit will not correct the outcome—at least a 90% chance (and typically much more) that the audit will correct the outcome. Thus, if the risk limit is 1%, then, in the long run at least 99 out of 100 wrong outcomes would be corrected by the audit.

The number of ballots required to conduct an RLA will vary based on the smallest margin of the contest selected and the risk limit. The smaller the margin, the more ballots to audit. The smaller the risk limit, the more ballots to audit.

Computer software cannot be guaranteed to be perfect or secure, so voting systems should be software-independent – An undetected change or error in voting system software should be incapable of causing an undetectable change or error in an election outcome. An RLA leverages software independence by checking the audit trail strategically. Efficient RLAs do not require complicated calculations or in-house statistical expertise.

An RLA software program is used to calculate the number of ballots to audit, randomly select the ballots, provide a ballot lookup table, and notify the user when the audit can stop. The audits depend on sampling methodology as well as statistical methodology. There are four types of sampling methodologies: ballot polling, ballot comparison, batch polling, and batch comparison. Additionally, there are two types of statistical methods: RLA and Bayesian.

In 2009, Colorado's HB 09-1335 introduced RLAs to commence with the 2014 General Election. In 2013, Colorado conducted the first pilot RLA at Arapahoe County. More counties were added in 2015-16. Colorado developed rules, procedures, and software to conduct an RLA for the 2017 Coordinated Election. The November odd-year election is generally referred to as the coordinated election. Coordinated elections are conducted by mail ballot.

In 2014, Cuyahoga County, Ohio, conducted a risk limiting audit for its gubernatorial race. Incumbent John Kasich received 51 percent of the votes cast in the county, and challenger Edward FitzGerald received 45 percent. The county Board of Elections needed to recount slightly more than 8,000 ballots before it could confidently determine that Governor Kasich had correctly been declared the winner. The board also audited the race for state treasurer, in which incumbent Joshua Mandel received 39 percent of the vote versus 61 percent for challenger Connie Pillich. In this less competitive contest, fewer than 2,500 ballots were needed to certify Pillich's victory among county voters.

The California secretary of state recently completed a three-year pilot program that audited contests of varying size in counties throughout the state.

In September 2017, Rhode Island became the second state to require risk limiting audits, for implementation by 2020, with possible pilots in 2018.

References

A Gentle Introduction to Risk-limiting Audits, by Mark Lindeman and Philip B. Stark, IEEE SECURITY AND PRIVACY, SPECIAL ISSUE ON ELECTRONIC VOTING, 2012.
https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

A Bayesian Method for Auditing Elections
https://www.usenix.org/system/files/conference/evtwote12/rivest_bayes_rev_073112.pdf

For more details please see the PowerPoint presentation by Jerome Lovato at the end of this document.

Marion County Post-Election Audit Pilot Agenda

Location: Election Service Center at 3737 E. Washington St., Indianapolis, IN 46201

Day 1 – May 29th 12:00 PM – 4:30PM

12:00 PM	VSTOP: Introductions
12:15 PM	County: Review state/county guidelines for handling ballots and accessing restricted areas
12:30 PM	County: Walk through procedure for organizing and storing ballots
1:00 PM	J. Lovato: Provide Risk Limiting Audit (RLA) overview to county officials (Q&A)
1:30 PM	Create/Review Ballot Manifests, organize ballots for audits
3:00 PM	Ensure Primary ballots are separated by Democratic and Republican categories, nonpartisan, if applicable
4:00 PM	Phone Conference with Secretary Lawson

Day 2 – May 30th 8:30 AM – 3:30 PM

8:30 AM	VSTOP: Introductions J. Lovato: Risk Limiting Audit overview Dr. Rivest: Bayesian Audit Method
9:15 AM	Ballot Polling Audit of 2016 Presidential Race in Precincts LA-03, WS-49, PE-39, WR-23 and WS-69
10:00 AM	Break
10:15 AM	Ballot Polling Audit of 2018 Republican U.S. Senate Race in Precincts PI-08, PI-09, PI-13, PI-19, LA-18, WR-28, WR-33, WR-35, WS-14 and WS-27
11:00 AM	Ballot Polling Audit of 2018 Democrat Marion County Sheriff in Precincts PI-08, PI-09, PI-13, PI-19, LA-18, WR-28, WR-33, WR-35, WS-14 and WS-27
Noon	Remarks by Secretary Connie Lawson
12:15 PM	Lunch Break
1:30 PM	Bayesian Audit of 2016 Presidential, 2018 Primary R-U.S. Senate Race 2018 Primary D-Sheriff Race
2:15 PM	J. Lovato: Example/demo of comparison audit procedures
3:00 PM	Conclusion

The RLA Pilot Team

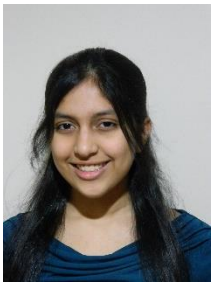
Jerome Lovato, Election Technology Specialist, U. S. Election Assistance Commission (EAC)

Jerome received his Bachelor of Science in Electrical Engineering from the University of Colorado at Denver. After working as an electrical engineer in the consumer electronics industry for six years, he worked as a Voting Systems Specialist at the Colorado Secretary of State's office for 10 years as a Voting System Certification Lead and Risk-Limiting Audit Project manager. Currently, he is an Election Technology Specialist for the U.S. Election Assistance Commission. Jerome led the team in Colorado that employed the RLA method. The following link is a gentle introduction to this method: https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

Dr. Ronald L. Rivest, Institute Professor at MIT

Professor Rivest is an Institute Professor at MIT. He joined MIT in 1974 as a faculty member in the Department of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and a founder of its Cryptography and Information Security Group. He is a co-author (with Cormen, Leiserson, and Stein) of the text, *Introduction to Algorithms*. He is also a founder of RSA Data Security, now named RSA Security (the security division of EMC), Versign, and Peppercoin. Professor Rivest has research interests in cryptography, computer and network security, electronic voting, and algorithms. A paper on the Bayesian method can be found at: https://www.usenix.org/system/files/conference/evtwote12/rivest_bayes_rev_073112.pdf

Mayuri Sridhar, Research and Innovation Scholar, MIT



Mayuri Sridhar is a Master's student studying Artificial Intelligence at MIT. She completed her undergraduate degree at MIT, double majoring in computer science and mathematics. Her research, under Professor Rivest's supervision, focuses on statistics and optimization, applied to election audits.

Marion County Clerk's Office

Myla A. Eldridge, County Clerk
Brienne Delaney, Director of Elections
Jenny Troutman, Deputy Director of Elections
Joanna Alexander, Absentee Administrator
Colin Claycomb, Ballot Administrator
Rhonda Hawkins, Service Center Manager
and other county staff personnel

The VSTOP Team

Dr. Jay Bagga and Dr. Bryan Byers, VSTOP Co-Directors
Jessica Martin, VSTOP Project Manager
Mani Kilaru, VSTOP IT Specialist
Molly Owens, VSTOP Graduate Assistant
Contact: VSTOP@bsu.edu

Statistical Post-Election Audit Pilot at Marion County, IN

Jerome Lovato, Election Technology Specialist
U.S. Election Assistance Commission

Let's talk about statistics-based post-election audits.

Indiana Post-Election Audit

IC 3-11-13-38

Petition for confirmation of vote cast

County Chairman

Petition

- 5% of precincts
  or
- 5 precincts

Constraints:

- Petition must be submitted between Saturday before election – Thursday after the election
- Applies only to ballot card voting system

County Election Board

Marion County Pilot

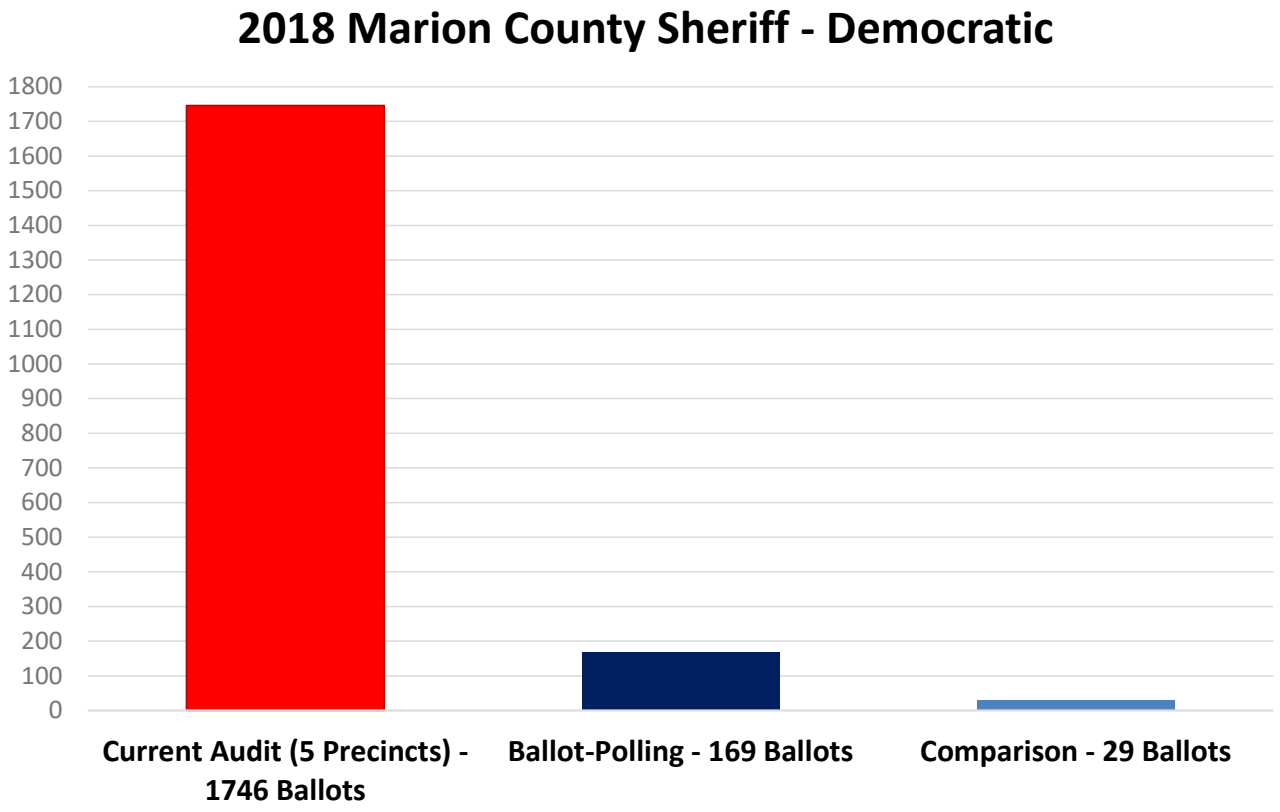
Marion County

Ballot-Polling RLA

Bayesian Audit

Comparison RLA

RLA Workload Example



Statistical Audit Methods - Terminology

A **risk-limiting audit (RLA)** provides strong statistical evidence that the election outcome is right, and has a high probability of correcting a wrong outcome.[1] There are two main types of RLAs: ballot-polling and comparison.

The **risk limit** is the largest chance that a wrong outcome will not be corrected. If the risk limit is 5% and the outcome is wrong, there is at most a 5% chance that the audit will not correct the outcome, and at least a 95% chance that the audit will correct the outcome.

A **Bayesian audit** is a statistical tabulation audit that provides assurance that the reported contest outcome is correct, or else finds out the correct contest outcome.[2]

A **Bayesian risk limit** is a desired upper bound on the probability that the audit will make an error (by accepting an incorrect reported contest outcome as correct).

Sampling Methodologies

Ballot Polling	Ballot Comparison	Batch Polling	Batch Comparison
• Randomly draw ballots • Examine ballots by hand • Tally results for each ballot	• Randomly draw ballots • Examine ballots by hand • Compare each ballot to its cast vote record (CVR)	• Randomly draw batches • Examine ballots by hand • Tally results for each batch	• Randomly draw batches • Examine ballots by hand • Tally results for each batch • Compare each batch to its batch report produced by the voting system

Statistical Methodologies

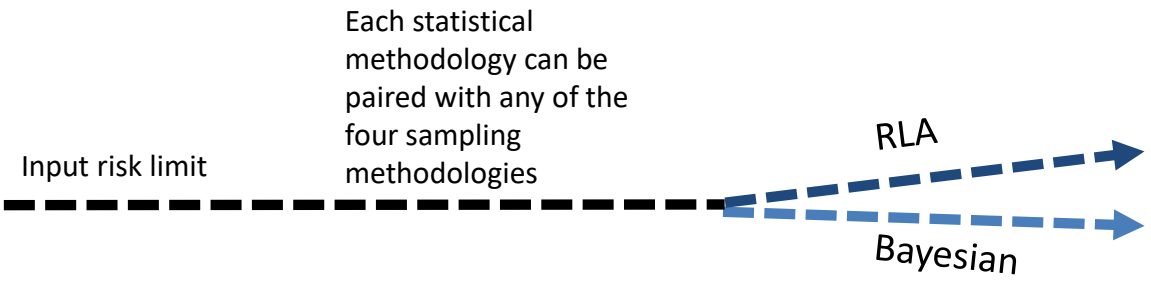
There are two statistical methodologies that describe how the statistical data obtained from the sampling methodologies will be used.

Risk-Limiting Audit

Bayesian Audit

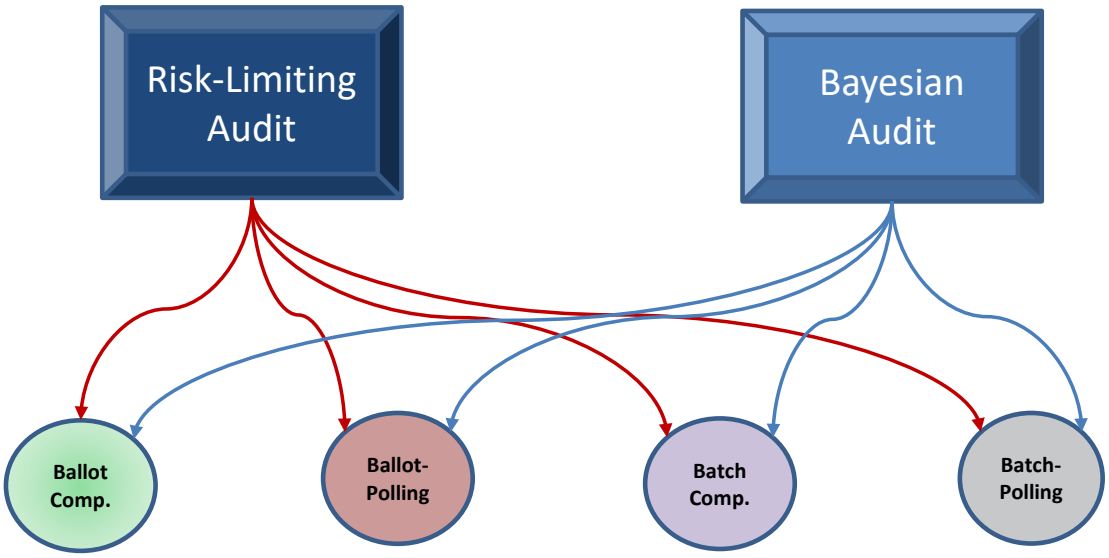
Statistical Methodologies Cont.

The statistical methodology determines whether the audit can stop, or whether more data needs to be obtained. The statistical assurances provided are slightly different between these two types.



Statistical Methodologies Cont.

There are at least eight different kinds of audits one may run, depending on the choice of sampling methodology and statistical methodology.



Statistical Methodologies Cont.

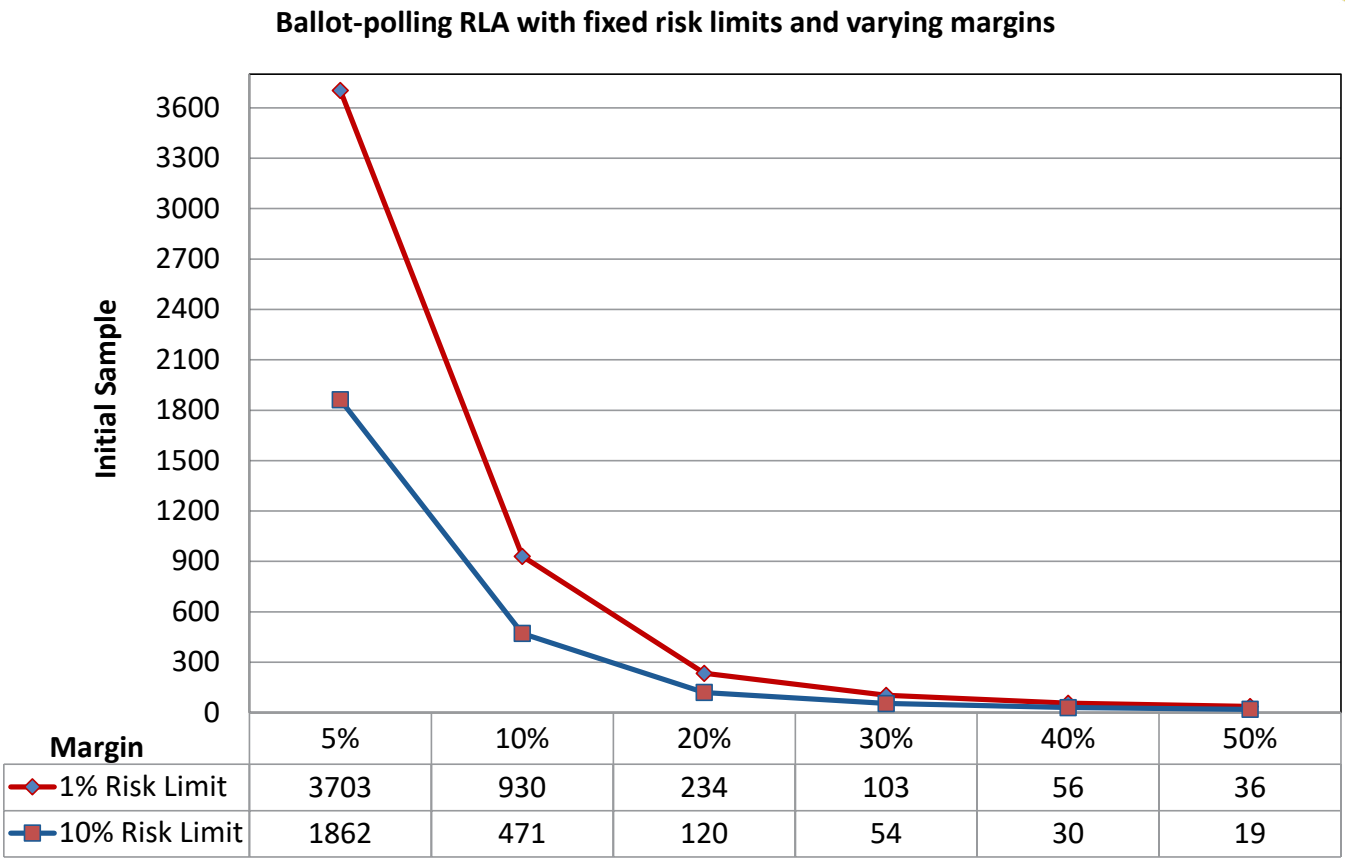
Comparison vs Polling	• Comparison is more efficient, but requires CVRs • Polling can be used if CVRs are not available
Ballot-Level vs Batch-Level	• Ballot-level audits are more efficient than batch-level since they require examining less ballots.
RLA vs Bayesian	• RLA is more popular and statistically rigorous • Bayesian is more flexible and can be used in non-standard situations

About Ballot-Polling RLAs

A ballot-polling RLA is similar to an exit poll. In this case, ballots (people) are randomly selected and tabulated (polled).

Pros	Cons
Minimal set-up costs	May require additional human resources
Does not require information from the voting system	Does not provide information about errors
Efficient for margins of 10% or greater	Inefficient for margins less than 10%

Ballot-Polling RLAs by the Numbers



About Bayesian Audits

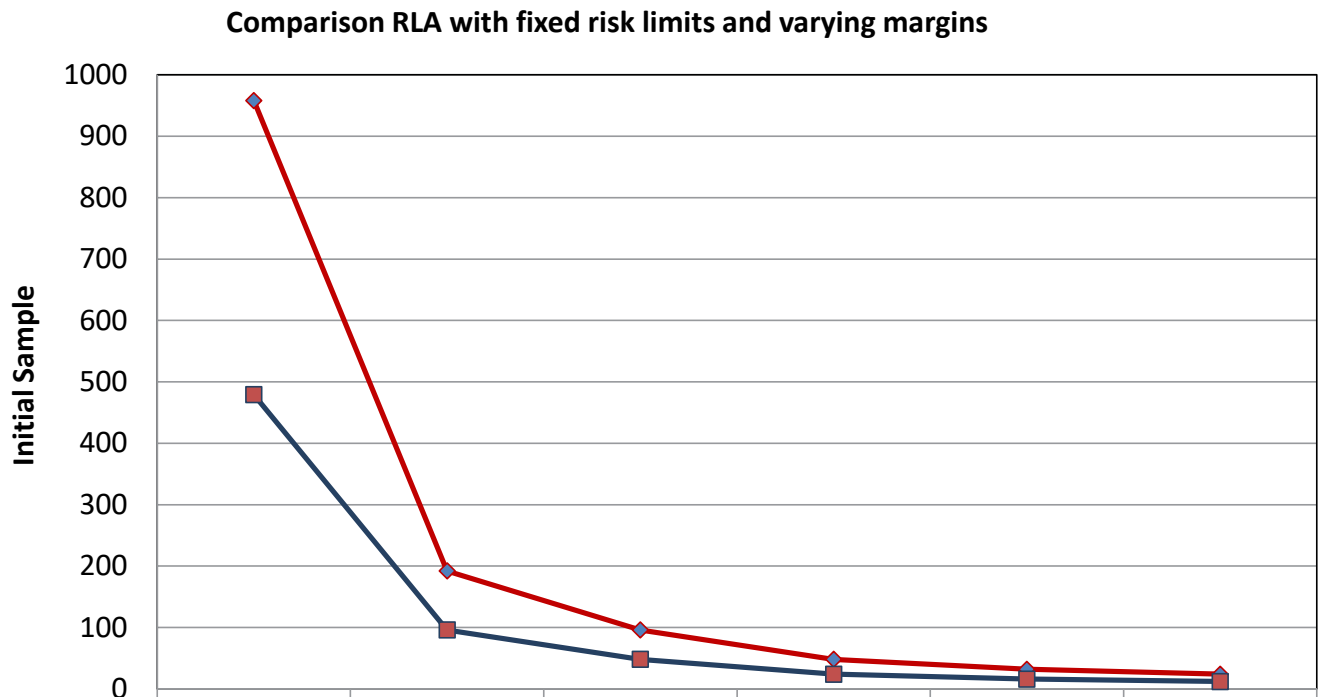
Pros	Cons
Automatically provides a measure of risk at each point	It is simulation-based and software dependent
Does not require information from the voting system	Costs are unknown
Efficient for cross-jurisdictional contests and other voting methods	Requires a level of trust from the public since the computations are not transparent

About Comparison RLAs

In a comparison RLA, individual ballots are randomly selected and compared to the CVR for each ballot.

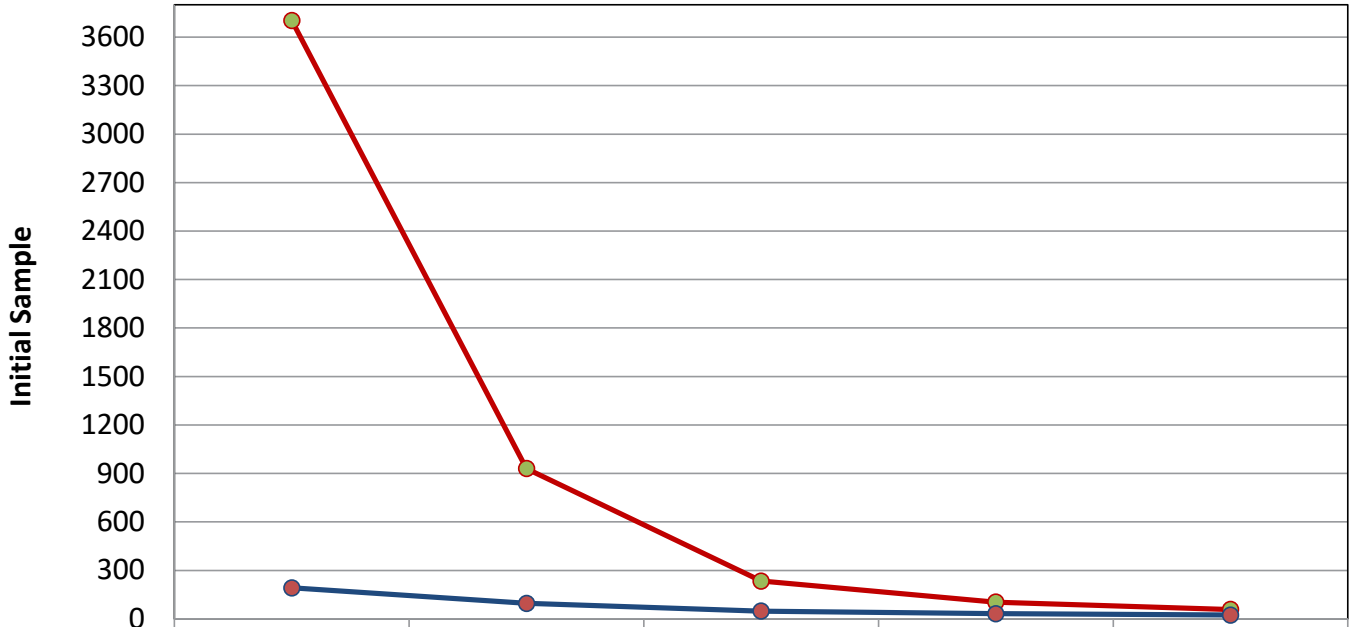
Pros	Cons
Requires fewer human resources to conduct an audit	Depends on a voting system that can produce a CVR
Allows the auditor to correct any errors	Retrieving specific ballots can be difficult and time consuming
Efficient for margins of any size	Requires maintaining ballots in the exact order they are scanned, or imprinting numbers on the ballots

Comparison RLAs by the Numbers



Margin	1%	5%	10%	20%	30%	40%
1% Risk Limit	958	192	96	48	32	24
10% Risk Limit	479	96	48	24	16	12

Ballot-Polling vs Comparison RLAs



Margin	5%	10%	20%	30%	40%
Ballot-Polling	3703	930	234	104	58
Comparison	192	96	48	32	24

Uniform Audit Procedures

The uniform procedures that apply to the audit methods used are:

1. Maintain documented chain-of-custody for all ballots cast.
2. Create a ballot manifest, which is a document that describes how ballots are organized and stored.
3. Determine the risk limit.
4. Determine what contest(s) will be audited.
5. Decide what other utilities (software, calculator, spreadsheets, etc.) will be used to calculate the number of ballots to audit, randomly select the ballots, provide a ballot lookup table, and notify the auditor when the audit can stop.
6. Obtain a CVR from the voting system (this is only used for comparison RLAs). A CVR is an export of data from the voting system showing how the voting system interpreted markings on every ballot.

Marion County Pilot Procedures

Ballot-Polling RLA

Use Dr. Stark's ballot-polling RLA tool[3] and the ballot manifest.

1. Enter the contest information
2. Enter a random seed for the pseudo random number generator
3. Obtain the initial sample of ballots to audit
4. Marion County election staff will:
    1. Select the ballots
    2. Hand tally the results for each ballot
5. Enter the hand tally results into the audit tool
6. If the risk limit is met then the audit will stop.
7. If the risk limit is not met then additional ballots will be selected.

Marion County Pilot Procedures Cont.

Bayesian Audit

Use Dr. Rivest's Bayesian audit tool[4] and the initial sample from the ballot-polling RLA.

1. Enter the sample of ballots obtained from the ballot-polling RLA into the Bayesian audit tool
    1. The Bayesian audit tool will compute the estimated probability of winning a full manual recount. Given a Bayesian risk limit of 5%, the Bayesian audit will stop when the auditor is at least 95% certain that the reported contest outcome is correct.

Marion County Pilot Procedures Cont.

<u>Comparison RLA</u>

Use Dr. Stark's comparison RLA tool[5] and the ballot manifest

1. Enter the contest information
2. Enter a random seed for the pseudo random number generator
3. Obtain the initial sample of ballots to audit
4. Marion County election staff will:
    1. Select the ballots
    2. Compared the selected ballots to their CVRs
5. If the risk limit is met then the audit will stop.
6. If the risk limit is not met then additional ballots will be selected.

Marion County Pilot Parameters

Risk Limit = 10%

Bayesian Limit = 5%

Contests to audit:

- 2016 Presidential
  - Estimated sample size (ballot-polling RLA) = 62
  - Estimated sample size (comparison RLA) = 18
- 2018 Republican U.S. Senate
  - Estimated sample size (ballot-polling RLA) = 242
  - Estimated sample size (comparison RLA) = 35
- 2018 Democrat Marion County Sheriff
  - Estimated sample size (ballot-polling RLA) = 169
  - Estimated sample size (comparison RLA) = 29

Sample Ballot Manifest

Precinct ID	Total # of Ballots	Precinct Batch ID	# of Precinct Ballots	Absentee Batch ID	# of Absentee Ballots
LA-03	400	LA-03P	300	LA-03A	100
WS-49	400	WS-49P	300	WS-49A	100
PE-39	600	PE-39P	400	PE-39A	200
WR-23	600	WR-23P	400	WR-23A	200
WS-69	600	WS-69P	400	WS-69A	200

What is Next?

- Conduct additional pilots at counties of different sizes that use different voting systems.
- Determine what entity will serve as the central audit authority.
- Determine what method(s) will best serve Indiana.
- Draft laws and procedures for conducting an audit.
- Train local election officials on how to conduct audits.

- **Implement a statistics-based post-election audit.**

Notes

1. The ballot-polling and comparison RLAs were developed by Dr. Philip Stark, Associate Dean, Division of Mathematical and Physical Sciences at University of California - Berkeley, and Dr. Mark Lindeman, Adjunct Assistant Professor of Political Science at Columbia University. These methods have been tested by various jurisdictions around the U.S., and were implemented by Colorado beginning with the November 2017 election. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

2. Dr. Ron Rivest, Institute Professor at MIT, developed the Bayesian audit method that will be tested for the first time in Marion County, Indiana. https://arxiv.org/pdf/1801.00528.pdf

3. Ballot-Polling RLA Tool: https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm#

4. Bayesian Audit Tool: http://audits.csail.mit.edu/

5. Comparison RLA Tool: https://www.stat.berkeley.edu/~stark/Vote/auditTools.htm#

Contact

Jerome Lovato
jlovato@eac.gov
(202)805-4613

Social media

Email
listen@eac.gov

Facebook
Facebook.com/eacgov1

Twitter
@EACgov

Youtube Channel
Election Assistance Commission

Website
www.eac.gov

Appendix B

Introduction:

This document reports the results of the RLA pilot conducted in Marion County, Indiana on May 29-30.

Marion County stores ballots by precinct ID (election day voted ballots (P), absentee (A) and unreadable (U)). There may be multiple absentee and/or unreadable batches (groups of ballots) differentiated by timestamps. We did not change this organizational structure for the audit. Rather, we adjusted the ballot manifests.

In the following, section 1 includes the implementation details for the 2016 General Presidential Race, section 2 covers the details for the 2018 Primary Sheriff Race (Democratic) and section 3 covers the details for the 2018 Primary U.S. Senate Race (Republican).

All the methods described below use an input seed (a random number with at least 20 digits). This input seed is used to begin the process of generating random numbers. In our case, this was achieved by rolling a 10-sided die which resulted in the input seed being 66286159831966888996. This input seed was used by Stark's RLA and Rivest's Bayesian method tools to generate a pseudo-random sample[2] of ballots.

The following risk limits (see Appendix A) were used for each audit:

- A Risk Limit of 10% for Stark's method
- A Bayesian Limit of 5% for Rivest's method

[2] https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

Section 1: Risk-Limiting Audit for the 2016 General Presidential Election

For this race, we selected five precincts (LA-03, WS-49, PE-39, WR-23 and WS-69). The candidates were Donald Trump, Hillary Clinton, Gary Johnson and Write-In. Ballot Polling was employed with two approaches (Stark's RLA and Rivest's Bayesian). The ballot polling procedure involved the following steps:

- Ballots were randomly drawn
- Ballots were examined by hand
- Results for each ballot were tallied

Creating Manifest:

Precinct ID	Total # of Ballots	Batch ID	# of Ballots in Batch
LA-03	400	LA-03P	295
		LA-03A 5:19PM	103
		LA-03U	1
		LA-03A 1:48 PM	1
WS-49	399	WS-49P	354
		WS-49A 6:12 PM	45
PE-39	600	PE-39P	510
		PE-39A Election Day	85
		PE-39U	4
		PE-39A Unknown	1
WR-23	604	WR-23P	506
		WR-23A 1:30 PM	94
		WR-23U	4
WS-69	599	WS-69P	444
		WS-69A 2:02 PM	149
		WS-69U	4
		WS-69A 10:23 PM	1
		WS-69A Unknown	1

Table 1: Manifest

Converting manifest to tool-readable format:

We copied and pasted the fields ("Batch ID (include timestamp if available)","# Ballots") into a notepad file.

Example:

Precinct: LA-03
"Batch ID (include timestamp if available)","#Ballots"
LA-03P, 295

Absentee Ballots:
"Batch ID (include timestamp if available)","#Ballots"
LA-03A 5:19 PM,103

Unreadable Ballots:
"Batch ID (include timestamp if available)","#Ballots"
LA-03U,1

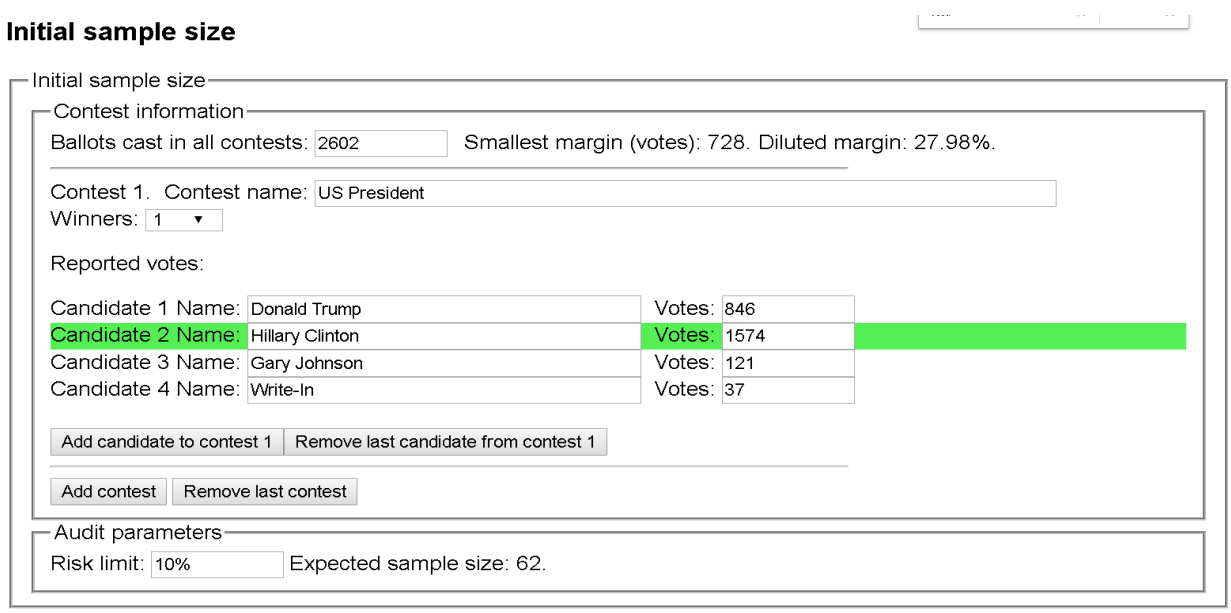
Output:

LA-03P,295
LA-03A 5:19 PM,103
LA-03A 1:48 PM,1
LA-03U,1
WS-49P,354
WS-49A 6:12PM,45
PE-39P,510
PE-39A Election Day,85
PE-39U,4
PE-39A Unknown,1
WR-23P,506
WR-23A 1:30 PM,94
WR-23U,4
WS-69P,444
WS-69A 2:02 PM,149
WS-69U,4
WS-69A 10:23 PM,1
WS-69A Unknown,1

Implementation:

Ballot Polling (Stark RLA Method):

The above fields were input into the tool https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm# The sample size of ballots was calculated by entering reported votes by candidate and total number of votes cast. Here the sample size was 62.



The seed number was input into the tool in order to generate a pseudo-random sample of ballots. The 'current sample number' field was initialized to 0. The fields 'Number of ballots' and 'Draw this many

ballots' are auto-initialized. The random ballot numbers were selected and sorted with duplicates removed when the draw sample button was clicked. In our case, 61 ballots were selected after removing duplicates.

Pseudo-Random Sample of Ballots

Seed: 66286159831966888996

Number of ballots: 2602

Current sample number: 62

Draw this many ballots: 62 draw sample reset

Ballots selected: ☑ show sequence numbers ☐ show hash values

The sorted sample ballots were examined by hand (audited) with the results as shown below:

Should more ballots be audited?

Audit progress

Audited votes for US President: 61		
Hillary Clinton	36	
Donald Trump	20	0.1
Gary Johnson	3	0
Write-In	2	0

Bayesian Method (Rivest's Method):

The Bayesian tool was initialized with the following fields:

Step 1: Enter Candidate Names

In the box below, enter the names of the candidates as a comma-separated list.

Example: `Alice, Bob`

Candidate names: Donald Trump, Hillary Clinton, Gary Johnson, Write-In

Step 2: Enter Number of Counties

In the box below, enter the number of counties being audited as a comma-separated list.

Example: 4

Number of Counties: 1

Step 3: Enter number of votes cast per county

In the box below, enter the total number of votes cast in each county. For multiple counties, separate entries with commas.

Single-county example: `101277`

Multi-county example: `101277, 231586, 50411`

Votes cast per county: 2602

Step 4: Enter tally for audit sample

In the box below, specify the tally for the sample drawn so far in the audit.

For a single county, just give a comma-separated list of numbers, one tally count per candidate, in the same order as the candidate names given above.

For multiple counties, separate the tallies for different counties with a semicolon. The county segments must be in the same order as used earlier for the county sizes.

Single-county example: `47, 62`

In this single-county two-candidate example, the audit has seen 47 votes for Alice and 62 votes for Bob.

Multi-county example: `47, 62; 101, 84; 17, 99`

In this multi-county (three-county two-candidate) example, the sample in county 2 had 101 votes for Alice.

Sample tallies by county: 20,36,3,2

(Optional) Specify random number seed

The computation uses a random number seed, which defaults to 1. You may if you wish enter a different seed here. (Using the same seed with the same data always returns the same results.) This is an optional parameter; there should be no reason to change it.

Seed: 6628615983196688896 6

BPTOOL (Bayesian ballot-polling tool version 0.8)

Candidate name	Estimated probability of winning a full manual recount
Clinton	98.34 %
Trump	1.66 %
Johnson	0.00 %
Write-In	0.00 %

Click here to go back to the main page.

After auditing 61 ballots, Stark's tool and the BP Tool reached the risk limits of 10% and 5%. This estimated the probability of Hillary Clinton winning the race without a full manual recount.

Section 2: Risk-Limiting Audit for the 2018 Primary Sheriff Election (Democratic)

For this race, we selected ten precincts (PI-08, PI-09, PI-13, PI-19, LA-18, WR-28, WR-33, WR-35, WS-14 and WS-27). The candidates were Bill Benjamin, Kerry Joseph Forestal and Undervote (for an RLA). The ballot selections were made using a combination of a Three-Cut and random sampling method. The Ballot Polling audit was conducted using two approaches (Stark's RLA and Rivest's Bayesian). The ballot polling procedure involved the following steps:

- Ballots were randomly drawn
- Ballots were examined by hand
- Results for each ballot were tallied

Creating Manifest:

Precinct ID	Total # of Ballots	Batch ID	# of Ballots in Batch
PI-09	198	PI-09P	189
		PI-09A 9:34 PM	9
		PI-09U	0
WR-35	195	WR-35P	184
		WR-35A 3:54 PM	11
WR-33	195	WR-33A 7:12 PM	1
		WR-33U	1
		WR-33P	181
		WR-33A 4:07 PM	12
PI-19	186	PI-19P	178
		PI-19A 5:04 PM	7
		PI-19U	1
PI-13	183	PI-13P	80
		PI-13A (A) A	27
		PI-13A (B) B	9
		PI-13A (C) C	25
		PI-13A (D) D	12
		PI-13A (E) E	8
		PI-13A (F) F	20
		PI-13U	2
WS-27	168	WS-27P	147
		WS-27A 3:40PM	21
WR-28	166	WR-28P	158
		WR-28A 1:10PM	8
PI-08	154	PI-08P	147
		PI-08A 9:50 PM	7
WS-14	154	WS-14P	134
		WS-14A 4:37 PM	20
LA-18	148	LA-18P	136
		LA-18A Unknown	12

Table 2: Manifest

Converting Table 2 to tool-readable format:

We copied and pasted the fields (“Batch ID (include timestamp if available)”,”# Ballots”) into a notepad file.

Example:

Precinct: PI-09
“Batch ID (include timestamp if available)”,”#Ballots”
PI-09P,189

Absentee Ballots:
“Batch ID (include timestamp if available)”,”#Ballots”
PI-09A 9:34 PM,9

Unreadable Ballots:
“Batch ID (include timestamp if available)”,”#Ballots”
PI-09U,0

Output:

PI-09P,189
PI-09A 9:34 PM,9
PI-09U,0
WR-35P,184
WR-35A 3:54 PM,11
WR-33A 7:12 PM,1
WR-33U,1
WR-33P,181
WR-33A 4:07 PM,12
PI-19P,178
PI-19A 5:04 PM,7
PI-19U,1
PI-13P,80
PI-13A (A) A,27
PI-13A (B) B,9
PI-13A (C) C,25
PI-13A (D) D,12
PI-13A (E) E,8
PI-13A (F) F,20
PI-13U,2
WS-27P,147
WS-27A 3:40PM,21
WR-28P,158
WR-28A 1:10PM,8
PI-08P,147
PI-08A 9:50 PM,7
WS-14P,134
WS-14A 4:37 PM,20
LA-18P,136
LA-18A Unknown,12

Implementation:

Ballot Polling: (Stark RLA Method)

The above fields were input into the tool https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm# The sample size of ballots was calculated by entering reported votes by candidate and total number of votes cast. Here the sample size was 169.

Initial sample size

Initial sample size

Contest information

Ballots cast in all contests: 1747 Smallest margin (votes): 293. Diluted margin: 16.77%.

Contest 1. Contest name: Sheriff

Winners: 1

Reported votes:

Candidate 1 Name: Bill Benjamin Votes: 692

Candidate 2 Name: Kerry Joseph Forestal Votes: 985

Add candidate to contest 1 | Remove last candidate from contest 1

Add contest | Remove last contest

Audit parameters

Risk limit: 10% Expected sample size: 169.

The seed number was input into the tool in order to generate a pseudo-random sample of ballots. The 'current sample number' field was initialized to 0. The fields 'Number of ballots' and 'Draw this many ballots' are auto-initialized. The random ballot numbers were selected and sorted with duplicates removed when the draw sample button was clicked. In our case, 155 ballots were selected after removing duplicates.

Random sampling

Pseudo-Random Sample of Ballots

Seed: 66286159831966888996

Number of ballots: 1747

Current sample number: 169

Draw this many ballots: 169 | draw sample | reset

The sorted sample ballots were examined by hand (audited) with the results as shown below:

Audit progress

Audited votes for Sheriff: 155

Kerry Joseph Forestal

85

Bill Benjamin

70

0.78

Once one has reached the sample number of ballots, if the risk limit is not met one continues the selection of ballots, using the three-cut method until the risk limit has been reached. In this case,13 more ballots were needed for Kerry Joseph Forestal to meet the risk limit.

Bayesian Method: (Rivest's Method)

The Bayesian tool was initialized with the following fields:

Step 1: Enter Candidate Names

In the box below, enter the names of the candidates as a comma-separated list.

Example: `Alice, Bob`

Candidate names: Bill Benjamin,Kerry Joseph Forestal,Undervote

Step 2: Enter Number of Counties

In the box below, enter the number of counties being audited as a comma-separated list.

Example: `4`

Number of Counties: 1

Step 3: Enter number of votes cast per county

In the box below, enter the total number of votes cast in each county. For multiple counties, separate entries with commas.

Single-county example: `101277`

Multi-county example: `101277, 231586, 50411`

Votes cast per county: 1747

Step 4: Enter tally for audit sample

In the box below, specify the tally for the sample drawn so far in the audit.

For a single county, just give a comma-separated list of numbers, one tally count per candidate, in the same order as the candidate names given above.

For multiple counties, separate the tallies for different counties with a semicolon. The county segments must be in the same order as used earlier for the county sizes.

Single-county example: `47, 62`

In this single-county two-candidate example, the audit has seen 47 votes for Alice and 62 votes for Bob.

Multi-county example: `47, 62; 101, 84; 17, 99`

In this multi-county (three-county two-candidate) example, the sample in county 2 had 101 votes for Alice.

Sample tallies by county: 70,85,5

BPTOOL (Bayesian ballot-polling tool version 0.8)

Candidate name	Estimated probability of winning a full manual recount
Forestal	89.32 %
Benjamin	10.68 %
Other	0.00 %

Click here to go back to the main page.

Once one has reached the sample number of ballots, if the Bayesian limit is not met one continues the selection of ballots, using the three-cut method until the Bayesian limit has been reached. In this case,10 more ballots were needed for Kerry Joseph Forestal to meet the Bayesian limit.

Section 3: Risk-Limiting Audit for 2018 Primary U.S. Senate Election (Republican)

For this race, we selected ten precincts (PI-08, PI-09, PI-13, PI-19, LA-18, WR-28, WR-33, WR-35, WS-14 and WS-27). The candidates were Mike Braun, Luke Messer, Todd Rokita and Other (includes undervotes and overvotes). A ballot comparison was employed for this race. This procedure involved the following steps:

- Ballots were randomly drawn
- Ballots were examined by hand
- Compare each ballot to its simulated cast vote record (CVR)

Creating Manifest:

Precinct ID	Total # of Ballots	Batch ID	# of Ballots in Batch
PI-09	156	PI-09P	152
		PI-09A 9:34 PM	4
WR-35	169	WR-35P	162
		WR-35A 3:54 PM	7
WR-33	127	WR-33P	118
		WR-33A 4:07 PM	9
PI-19	120	PI-19P	113
		PI-19A 5:04 PM	7
PI-13	197	PI-13P	52
		PI-13A (a) a	25
		PI-13A (b) b	21
		PI-13A (c) c	26
		PI-13A (d) d	28
		PI-13A (e) e	12
		PI-13A (f) f	31
		PI-13U	2
WS-27	141	WS-27P	126
		WS-27A 3:54 PM	15
WR-28	124	WR-28P	122
		WR-28A 1:10 PM	2
PI-08	170	PI-08P	155
		PI-08A 9:50 PM	15
WS-14	167	WS-14P	154
		WS-14A 4:37 PM	12
		WS-14U	1
LA-18	119	LA-18P	114
		LA-18A Unknown	5

Table 3: Manifest

Implementation:

The total number of ballots for this race was 1,490. However, due to time limitations, we elected to restrict the population size by randomly selecting 30 ballots using the Three-Cut method. This group of ballots was then treated as the population from which 16 ballots were selected for the sample using the Three-Cut method.

Initial sample size

Initial sample size

Contest information

Ballots cast in all contests: 30 Smallest margin (votes): 9. Diluted margin: 30%.

Contest 1. Contest name: Senate

Winners: 1

Reported votes:

Candidate 1 Name:	Mike Braun	Votes:	16
Candidate 2 Name:	Luke Messer	Votes:	5
Candidate 3 Name:	Todd Rokita	Votes:	7
Candidate 4 Name:	Other	Votes:	2

Add candidate to contest 1 | Remove last candidate from contest 1

Add contest | Remove last contest

Audit parameters

Risk limit: 10%

Expected rates of differences (as decimal numbers):

Overstatements.	1-vote:	0.001	2-vote:	0.0001
Understatements.	1-vote:	0.001	2-vote:	0.0001

Starting size

Round up 1-vote differences. Round up 2-vote differences. Calculate size 16.

Output:

Stopping sample size and escalation

Ballots audited so far: 16

1-vote overstatements:	1	Rate: 0.0625
2-vote overstatements:	0	Rate: 0
1-vote understatements:	0	Rate: 0
2-vote understatements:	0	Rate: 0

Estimated stopping size

Calculate Audit incomplete

If no more differences are observed: 21.

If differences continue at the same rates: 21.

Estimated additional ballots if difference rates stay the same: 0.

According to the algorithm, at least 21 more ballots would need to be selected before it met the risk limit. This led to an effective recount of the 30 ballots in our full population of ballots. The recount did not contradict the certified outcome.

Conclusions:

For the 2016 Presidential race, after auditing sample ballots, the Stark's tool and the BP Tool reached the risk limits of 10% and 5%. This estimated the probability of Hillary Clinton winning the race without a full manual recount.

For the 2018 Primary Democrat Sheriff race, after auditing sample ballots, the Stark's tool and the BP Tool failed to reach the risk limits. In this case, 13 more ballots for Stark's tool and 10 more ballots for BP tool were needed to verify Kerry Joseph Forestal as a winner. However, these audits were ceased early due to time constraints.

For the 2018 Primary Republican U.S. Senator race, simulated CVRs were used for comparison. Due to time limitations, we elected to restrict the population size by randomly selecting 30 ballots using the Three-Cut method. This group of ballots was then treated as the population from which 16 ballots were selected for the sample using the Three-Cut method. The audit ceased early but did not contradict the election outcome for Mike Braun as the winner.

Appendix C

Observation of Denver County Primary 2018 Risk-Limiting Audit (RLA)

By Jessica Martin, Voting System Technical Oversight Program (VSTOP), Project Manager

Risk Limiting Audits (RLAs) are becoming more popular in Election Administration and in some States they are now legally required. As a former Election Coordinator in a county that prevalently used DRE (Direct Recording Electronic) devices, I had a lot of trepidation and questions about the trending usage of RLAs. Below is my report of what I learned from attending the RLA for the June 26, 2018 Primary Election in the State of Colorado.

When I arrived on Thursday July 5th, I was expecting to see a flurry of activity as 9:00am – 5:00pm was listed as wrapping up the tabulation of ballots, organizing/storage of ballots and county data entry into the state RLA tool. However, the bulk of this work had already been done and the County of Denver had graciously left a few items over so they could demonstrate this process from 4:00pm – 5:00pm to benefit those of us who had traveled for this event. The state requires that all ballot manifest information be entered in the RLA tool the evening before the audit seed is selected.

Colorado has 64 counties and the only counties which did not participate in the Primary RLA were the three counties that tabulated their results by hand. On Friday July 6th, at 9:00am the Secretary of State held a public meeting where he (and a number of volunteers) rolled a 10 sided die a total of 20 times to create the random seed. By 9:36am all Counties were able to go directly to the tool to see which ballots had been selected. In addition, counties receive an email with this information. From this time until the ballot selection occurred, the County was conducting work behind the scenes to ensure that ballot pulling would go off without a hitch. Unfortunately, much of this I did not get to see, but I thought it was important to note that each box of ballots was labeled with which ballots needed to be retrieved to ensure that teams retrieve those ballots in a single visit to the box. Copies of actual ballots were left as place markers.

The majority of counties, including Denver County where I visited, completed a comparison audit. A comparison audit requires that the County's voting system have the ability to organize and disseminate case vote records (CVR) appropriately. In contrast, when we did the Marion County, Indiana RLA they were not sure of the process and tools needed to connect the EVS 5.2.0.0 marked ballots and CVRs without contacting the vendor for assistance. In Denver County the ballots are imprinted with their corresponding CVR. An image of the imprint number on a copy of the ballot can be seen below (see Image 1). Although imprinting isn't the only method to connect the ballot to the corresponding CVR, being able to tie the ballot with the correct CVR is a necessity for a comparison RLA.

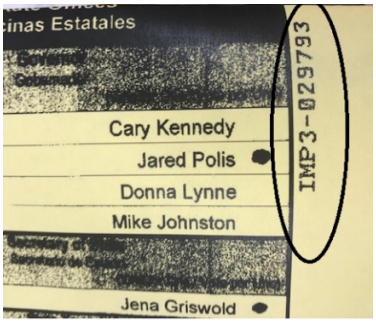


Image 1

After an election, the Secretary of State selects two races for each County (one statewide and one countywide) and then also determines the risk limit. This year the risk limit for comparison audits was 5% and the ballot polling risk limit was 10%. When asked which races are selected, it was noted that if the County Clerk and Secretary of State race are on the ballot then they are typically chosen.

When a ballot is pulled from a batch to be audited, a photocopy of the ballot image is left in its place. The pulling of ballots is an activity that involved multiple bipartisan teams of two, who would seal and unseal boxes and search through folders within those boxes. In addition, this all occurs in a secure room that is under video surveillance. The pulling of ballots is very methodical and organized. In the rare case a ballot is not found, the process is to enter into the RLA tool that the ballot was not found and the software treats this as a fail.

Once all of the ballots had been pulled a bipartisan team of one Republican Judge and one Democrat Judge confirmed every ballot was entered correctly into the tool. If there is a question about how a ballot was marked, there is an adjudication reference guide (see Image 2) that can be used to resolve the question. If the judges still disagree on a vote there is an option for "no consent."

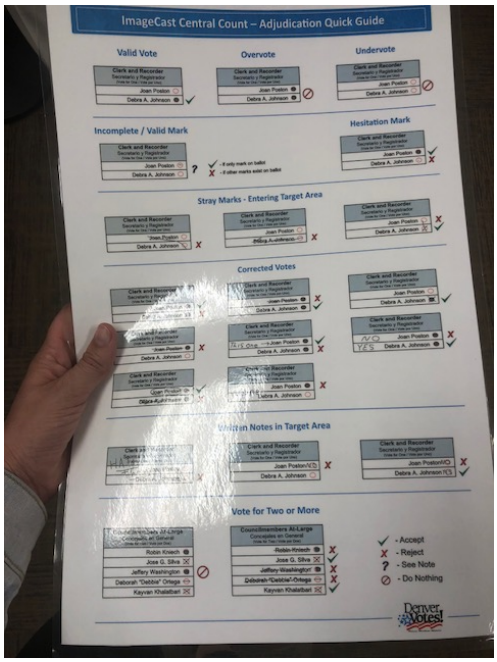


Image 2

Although only two races were chosen to be audited, all of the races voted on in the selected ballot are entered into the tool that collects the results of each ballot. The reason behind this is to collect as much data as possible.

The entry of data in the RLA tool appeared to be the most time consuming portion as we only had one person entering the data and one team of judges confirming that it was correct. Nonetheless, it was a very efficient process and was completed in the timeline allotted by the Office of the Secretary of State. If the first round of the ballot comparison audit had not met the risk limit, Denver County would have gone onto a second round. In this case, a second round of auditing was not needed and Denver County successfully completed the audit.

My observation of the RLA in Denver County alleviated my fears regarding ballot security, disorganization and undue administrative burden on the County that I previously had. I appreciated the opportunity to see Denver County's RLA, and I feel much more prepared to manage an RLA project in the future if appropriate. I saw a lot of similarities and differences between our pilot RLA in Marion County and Denver County's Primary 2018 RLA. The main difference is that much of Colorado's activities were automated and with software tools, whereas for Marion County a lot of our work was done manually via excel. Another difference was some of the laws currently in Colorado around conducting RLA's and canvassing dates and that ballots are open records.

Schedule of Events

COLORADO RISK-LIMITING AUDIT – 2018 PRIMARY ELECTION		
Day/date	**Events**	**Location**
Thursday, July 5th 9am – 5pm (est.)	• Counties finish tabulating ballots, enabling observers to watch how county officials organize and store paper ballots for retrieval during RLA • Counties export, hash and upload ballot manifests and cast vote record (CVR) files to Secretary of State via RLA software tool	Denver Elections Division 200 West 14th Avenue, Ste. 100 Denver, CO 80204
Friday, July 6th 9 am – 12 pm	• Secretary of State convenes a public meeting to establish 20-digit random seed by sequential rolls of 10-sided dice; the random seed is then utilized in the RLA software's pseudo-random number generator (PRNG) to randomly select ballots in each county for examination during the RLA • After public meeting adjourns, Secretary of State staff will demonstrate for observers how each county's audit is defined and launched using the RLA software	Colorado Secretary of State 1700 Broadway, 3rd Floor Denver, CO 80290
Friday, July 6th (afternoon) 2 pm – 5 pm (est.)	• Once the Secretary of State defines and starts each county's audit, the RLA software generates a list of ballots that each county audit board must examine • Each county downloads the list of randomly selected ballots, and bipartisan teams of election judges then locate and retrieve those specific ballots from storage containers	Denver Elections Division
Saturday, July 7th 9:00 am – 12:00 pm (est.)	• Bipartisan county audit boards begin the audit in earnest, and report voter markings from randomly selected ballots into RLA software • At conclusion of first round, RLA software compares the audit boards' reports to the corresponding cast vote record (CVR) for each audited ballot. • RLA software identifies any discrepancies between human and machine tabulations, and determines whether the risk limit is satisfied or an additional round of auditing is required.	Denver Elections Division

Resource

Audit Center Colorado Secretary of State by Wayne Williams
https://www.sos.state.co.us/pubs/elections/auditCenter.html

Acknowledgement

My gracious hosts at the Colorado Secretary of State Office and Denver County Elections Division who answered my abundant list of questions, sometimes before I even asked them.

APPENDIX D.5
ENERGY COMMITTEE

ENERGY COMMITTEE STRATEGIC PLAN

Chair: Mark Maassel | Co-Chair: Bob Richhart

September 2018
Indiana Executive Council on Cybersecurity

Energy Committee Plan

Contents

Committee Members **4**
Introduction **6**
Executive Summary **8**
Research **10**
Deliverable: Critical Infrastructure Information **15**
General Information 15
Implementation Plan 17
Evaluation Methodology 20
Deliverable: Training **22**
General Information 22
Implementation Plan 23
Evaluation Methodology 28
Deliverable: Contacts **30**
General Information 30
Implementation Plan 31
Evaluation Methodology 34
Deliverable: Coordinate with Others **36**
General Information 36
Implementation Plan 38
Evaluation Methodology 41
Deliverable: Metrics **43**
General Information 43
Implementation Plan 44
Evaluation Methodology 48
Supporting Documentation **49**
American Public Power Association (APPA) Cyberseucirty and the Electric Sector 50
Electricity Subsector Coordinating Council (ESCC) Brochure 53
Federal Energy Regulatory Commission (FERC) Critical Energy/Electric Infrastructure Information (CEII) Regulations 58
IECC Energy Committee Annual Metrics Report 61
IECC Energy Committee Commonwealth of Virginia (CoV) Briefing 63
National Conference of State Legislatures (NCSL) State Efforts to Protect the Electric Grid. 66

Committee Members

Committee Members

Name	Organization	Title	Committee Position	IECC Membership Type
Mark Maassel	Indiana Energy Association (IEA)	President	Chair: Full Time	Voting
Bob Richhart	Hoosier Energy	Vice President	Co-Chair: Full Time	Advisory
Scott Bowers	Indiana Electric Cooperatives (IEC)	Vice President	Full Time	Advisory
Carolyn Wright	IN Municipal Power Agency (IMPA)	Vice President	Full Time	Advisory
Kurt Aikman	Midcontinent Independent System Operator (MISO)	Manager	Full Time	Advisory
Walt Grudzinski	Vectren	Director	Full Time	Advisory
Stan Partlow	American Electric Power (AEP)/Indiana Michigan Power (I&M)	VP & Chief Security Office	Full Time	Advisory
Curtis Taylor	Wabash Valley Power Authority (WVPA)	VP, Technical Services	Full Time	Advisory
Scott Berry	IMPA	Manager, Environmental & NERC Compliance	Full Time	Advisory
Greg Ellis	Indiana State Chamber	VP	Full Time	Advisory
Paul Mitchell	Energy Systems Network (ESN)	President	Full Time	Advisory
Brain Rockensuess	Indiana Department of Environmental Management (IDEM)	Chief of Staff	As needed	Advisory
Sarah Freeman	Indiana Utility Regulatory Commission (IURC)	Commissioner	As needed	Voting Proxy
Jennifer deMedeiros	AES/ Indianapolis Power & Light (IPL)	Manager	As needed	Advisory
Allen Brown	Midwest Natural Gas	Director	Contributing	Advisory
Carl Cahill *	Duke Energy	Director	Contributing	Advisory
Chad Connell	MISO	Manager	Contributing	Advisory
Scott Miller	Citizens Energy Group	Manager	Contributing	Advisory

- Carl retired in early 2018 but was a Contributing Member of the Committee until he retired.

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Assessed national regulations and cybersecurity guidelines
  - Assessed what Subsector Cybersecurity Coordinating Councils exist and their level of activity
  - Assessed the presence and value of sector-specific Information Sharing and Analysis Center (ISAC).
  - Needs for training by educational institutions to provide cybersecurity professionals
  - Level of interaction, and need for interaction, with other subsectors'
  - Level of understanding of state priorities and response in a cyber emergency
  - Assessed what information is needed from other Committees/Work Groups on the Council

- **Research Findings**
  - The North American Electric Reliability Council (NERC) and Federal Energy Regulatory Commission (FERC) have set regulations on the electric utility industry. These are mandatory, and fines can be levied. The U.S. Transportation and Safety Administration (TSA) has Pipeline Security guidelines for natural gas utilities.
  - The electric utility industry, along with the nuclear industry, are the only critical infrastructure sectors which have mandatory, enforceable federal regulations in place for cybersecurity.
  - There is in place at the national level an Electric Subsector Coordinating Council and an Oil & Natural Gas Subsector Coordinating Council. Both are quite active.
  - Electric ISAC and Downstream Natural Gas ISAC are active.
  - Significant need for education and training exists.
  - There is a need to interact with other subsectors, including for example Telecommunications and Financial.
  - The Energy Committee believes a much clearer understanding of state priorities and responses in a cyber emergency would be important.

- **Committee Deliverable**
  - Critical Infrastructure Information Training
  - Contacts
  - Coordinate with Others
  - Metrics

- **Additional Notes**
  - None

- **References**
  - None

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. The electric and natural gas utility industry recognizes that the production, transmission, and distribution of electricity and natural gas is critical to the economy and well-being of Hoosiers, indeed for Americans. This industry is also heavily regulated, including in the cybersecurity arena. As a result, the industry has invested heavily to increase staffing, train employees, adopt the National Institute of Standards and Technology (NIST) framework and participate in tabletop exercises. An example of the training and exercise activities in which the industry participates is Grid-Ex. Grid-Ex is a biannual, nation-wide exercise which provides utilities a chance to "experience" a cyberattack. In 2017, the exercise included both electric and natural gas utilities as well as cyber and physical attacks.
    b. At the national level, an Electric Subsector Coordinating Council (ESCC) and Oil & Natural Gas Subsector Coordinating Council were created to formalize communications between government and utilities. In addition, the Energy Information Sharing and Analysis Center (E-ISAC) is a sector-specific information sharing clearinghouse that also includes downstream natural gas distribution companies such as those operating in Indiana. The E-ISAC provides threat information and analysis. Separately, a Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC) is a leading threat information and analysis resource for natural gas utilities operating in Indiana.

2. **What (or who) are the most significant cyber vulnerabilities in your area? Are these components cybersecure?**
    a. Cyber vulnerabilities of components that are purchased and then installed in the energy network.
    b. Need to improve communications between sectors on such things as threats which are detected by another sector.
    c. A common clearinghouse which assesses vendors with differing levels of cyber exposure and risk mitigation.
    d. Potential disruptions of the telecommunications networks.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. There is a significant need to enhance the educational capabilities in Indiana to train and educate individuals to work in cybersecurity.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Electric utilities are required to meet standards set by the North American Electric Reliability Council (NERC) and adopted by the Federal Energy Regulatory Commission (FERC). FERC regulations are binding and have the force of law. These standards have led to utilities adopting the NIST framework and implementing strong cybersecurity protocols, procedures and processes. The natural gas utilities work closely with the U.S. Transportation & Safety Administration (TSA). TSA has in place Pipeline Security Guidelines and is working with the industry to revise and update these guidelines.

5. **What case studies and/or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Both electric and natural gas facilities are a part of a national network. As such, issues are addressed recognizing that a cyberattack may impact large geographic areas and would not be limited to a single state. Electric utilities have conducted biennial exercises to test responses to such a large scale outage. These are named Grid-Ex. Grid-Ex IV was conducted in November 2017. It involved the electric and natural gas industries and tested responses to a cyberattack.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc.**
    a. Attached are several documents, which provide more details on these issues. (See Supporting Documentation)

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Since energy companies are all required to meet the same regulations or guidelines, training in the energy industry is reasonably similar across the country. And, as noted above, in addition to more localized exercises, energy utilities engage in national exercises as well.

8. **What does success look like for your area in one year, three years, and five years?**
    a. One Year
        1. Obtain a clearer understanding of state priorities in an emergency, including how the Public Sector plans to allocate scarce resources.
        2. Further development of curriculum at Indiana educational institutions to develop individuals for employment in cybersecurity.
        3. Development of a process to share threat information across and between sectors.
    b. Three Years
        1. Utilities have, if needed, modified plans to reflect Public Sector priorities.
        2. Utilities can begin to hire well trained and educated cybersecurity professionals.
        3. Robust information sharing processes have become standard operating procedure.
        4. Appropriate involvement of others on the Council in Grid-Ex, including observers.

c. Five Years
    1. Ongoing evolution of the way we work together in Indiana has revised and changed the way we work as we respond to the ever-changing risk environment.
    2. Utilities have an ever-increasing number of graduates from Indiana educational institutions who can work on cybersecurity issues.

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

a. As mentioned above, Indiana's educational institutions should be more intentional about training students for cybersecurity roles. Increased awareness of the importance of these roles and the types of jobs available in the field is needed.

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. Total Workforce
    - Over 12,000 direct employees.

b. Cybersecurity-related workforce
    - Over 45 employees. However, this number is not reflective of the total number of employees focused on cybersecurity in the utility industry which serves Indiana customers. Several companies who serve significant numbers of Hoosiers have consolidated their cybersecurity efforts into enterprise-wide departments. Since the utility industry operations cross state boundaries, this allows companies to consider cyber risks and address those risks across a much larger footprint. Considering all of these employees, would show employment of several hundred individuals.

c. Unmet cybersecurity-related workforce
    - While not a comprehensive assessment, each cybersecurity operation in the utility space would benefit from an increase in trained cybersecurity professionals.

11. What do we need to do to attract cyber companies to Indiana?

a. Vendors who work to address the issues raised in item 2a) and 2c) above in the Energy Committee Strategic Plan are areas for new companies to focus. Encouraging a robust business climate where new companies working to meet the needs of Indiana businesses can prosper is important.

12. What are your communication protocols in a cyber emergency?

a. Utilities operating in Indiana have established emergency operations centers for their companies. Individuals staffing these centers will be able to assess the nature of an incident and develop appropriate responses. These centers are also capable of communicating with other emergency operations centers. Communication protocols also include integrating the information from the Electric Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council.

13. What best practices should be used across the sectors in Indiana?

a. We will be better able to provide thoughts on this issue once we learn more about what already exists in the other sectors. Clearly, the electric and natural gas industries have benefited from participation in Coordinating Councils and the sector-specific ISACs. Broadening the flow of information from one sector to another would seem, at least on a preliminary basis, as an area ripe for implementation.

Deliverable: Critical Infrastructure Information (CII)

Deliverable: Critical Infrastructure Information

General Information

1. **What is the deliverable?**
    a. Review potential policy changes to protect critical infrastructure information while maintaining public access and freedom of information.

2. **What is the status of this deliverable?**
    a. 100 % Complete

3. **Which of the following IECC goals does this deliverable meet?**

☒ Establish an effective governing structure and strategic direction.
☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
☐ Strengthen best practices to protect information technology infrastructure.
☐ Build and maintain robust statewide cyber-incident response capabilities.
☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**

☐ Research – Surveys, Datasets, Whitepapers, etc.
☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
☒ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The Energy Committee is aware of the numerous existing rules and guidelines which already impact how electric and natural gas energy companies address cyber issues. Additional laws, regulations or policies will certainly increase the work required, potentially without increasing cybersecurity and with the potential to create conflicting laws, regulations or policies. We do not believe that additional laws or policies are needed in Indiana. We will monitor this issue since others may have ideas that warrant review by this Committee.

6. **What metric or measurement will be used to define success?**
    a. The electric and natural gas companies need a stable policy environment which provides flexibility to adapt to the ever-changing attacks. In particular, a consistent set of policies is important without conflicting provisions or policies which place activity above assuring security are needed. Finally, this industry is strongly interconnected across state lines. Hence, existing regulation is often appropriate to avoid conflicting requirements. Success will be measured by assuring consistent, flexible policies most likely implemented at the federal level.

7. **What year will the deliverable be completed?**
    a. 2018
    b. Rules have been in place for Indiana's energy sector members for almost 10 years.

8. **Who or what entities will benefit from the deliverable?**
    a. Customers, energy companies, law enforcement, disaster response personnel, media, and many others.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. At this point, there is not a notable or problematic overlap.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. We believe that the electric and natural gas operating environment is unique in having already put in place mandatory regulations and/or guidelines which impact companies across the nation as well as here in Indiana. We would anticipate that other members of the IECC may determine that policy level changes are needed. There may be lessons to be learned by others from reviewing the long-standing regulations and guidelines established by the NERC or the TSA. We will engage with other committees/working groups and attempt to accomplish their goals without impeding this industry's ability to implement strong cybersecurity programs.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Given the pervasive use of electricity and natural gas by almost all Hoosiers, it becomes important to interface with virtually all other sectors. However, among the most critical will be the US Department of Energy (DOE), Department of Homeland Security (DHS), TSA and FERC; the Indiana Department of Homeland Security (IDHS) and Utility Regulatory Commission (IURC); the NERC as well as Congress and the Indiana General Assembly. Similarly, law enforcement will need to be involved, whether that is the Federal Bureau of Investigation (FBI) or the Indiana State Police (ISP); lest they be overlooked, all aspects of the energy industry, including those represented on the IECC Energy Committee, will need to be involved.

12. Who should be main lead of this deliverable?

a. The Energy Committee is structured so that information flows to Mark Maassel at the Indiana Energy Association. It is his responsibility to share the information with the Energy Committee and to provide feedback to others

13. What are the expected challenges to completing this deliverable?

a. We believe that the only challenge, with consideration the IECC is set up in a manner that helps address the challenge, is the flow of information between and among IECC Committees and/or Working Groups.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Critical Infrastructure Information (CII) in the energy industry is defined by federal entities.	FERC and the TSA	100%	Complete	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
No additional staffing is required					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Consistent definition of CII occurs in the highly interconnected network of electric and natural gas facilities which reach across state lines.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Efficient communications as well as protecting key assets and information from "bad actors" will reduce cyber risk. These costs are already a part of operating our utilities. We do anticipate that costs will rise as the issues mature and become more challenging.

19. What is the risk or cost of not completing this deliverable?

a. This deliverable is already completed.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. CII definitions are in place and are being used. These have been in place and their use will continue into the future.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The cost of using the CII definitions are already a part of the energy industry cost structure.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. These supports are already in place within the energy utilities operating in Indiana.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. These definitions of CII have already been implemented within the utility sectors. An example of the definitions appears in the Energy Committee Strategic Plan. These definitions were taken from the FERC website and can be reached at the following hyperlink. https://www.ferc.gov/legal//maj-ord-reg/land-docs/ceii-rule.asp

27. Can this deliverable be used by other sectors?

a. Yes
b. Use by others may be possible; however, utilities are highly technical with unique operational characteristics and we suspect that not all definitions will translate well to other sectors.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. These are existing at the moment and have been implemented. Information has been shared by the industry. However, to the extent that others are not aware of this, they can contact the Energy Committee.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. While others are much better positioned and informed to answer this question, we do not necessarily see this item as a key for either public relations or marketing consideration.

Evaluation Methodology

Objective 1: IECC Energy Committee will provide current definitions and review of potential policy changes to protect critical infrastructure information while maintaining public access and freedom of information by July 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Training

Deliverable: Training

General Information

1. **What is the deliverable?**
   a. Determine the need to establish a training program.

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☒ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Our deliverable is to support others with a clear understanding of what this industry needs in training and education to support and enhance energy company cybersecurity.

6. **What metric or measurement will be used to define success?**
   a. This is likely best done by committee/task force that is focused on these issues. We are prepared to support their efforts as needed. The Workforce Development Committee responded to a question from this Committee that they will propose the formal adoption of the NICE framework by the IECC. This Committee supports the adoption of the NICE framework.

7. **What year will the deliverable be completed?**
    a. 2023+
    b. We would hope for progress in each of the upcoming years but acknowledge that the industry is evolving rapidly, and educational efforts will also be changing.

8. **Who or what entities will benefit from the deliverable?**
    a. All aspects of those involved directly in cybersecurity will benefit from an increasing pool of talented cyber experts, including organizations outside of Indiana.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Unknown.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. We will support other committees/working groups as they develop their plans. We anticipate that all committees of the Council will need to be a part of defining what is needed to train individuals to work in cybersecurity.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. This will be best defined by the Committees and Working Groups who are directly developing the needed training.

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Mark Maassel at the Indiana Energy Association. It is his responsibility to share the information with the Energy Committee and to provide feedback to others.

13. **What are the expected challenges to completing this deliverable?**
    a. This will be best defined by the Committees and Working Groups who are directly developing the needed training.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
The Energy Committee believes that a training program with certifications as well as college level and advanced degrees, providing initial and ongoing reskilling opportunities is needed. This should be focused around the NICE standards.	Workforce Development Committee	100% (The Energy Committee work of identifying the need is complete. We are prepared to support the Workforce Development Committee as they proceed forward.) [1]	Complete	
Develop and promote Certified Hacker Training Program.	Workforce Development Committee	100% (The Energy Committee work of identifying the need is complete. We are prepared to support the Workforce Development Committee as they proceed forward.) [1]	Complete	
Develop apprenticeship programs to help individuals who are entering the Cybersecurity field develop their skills and gain "real world" experience.	Workforce Development Committee	100% (The Energy Committee work of identifying the need is complete. We are prepared to support the Workforce Development Committee as they proceed forward.) [1]	Complete	
When individuals first begin to receive training, teach secure coding early on, perhaps even before teaching coding.	Workforce Development Committee	100% (The Energy Committee work of identifying the need is complete. We are prepared to support the Workforce Development Committee as they proceed forward.) [1]	Complete	

[1] The IECC Energy Committee is comprised of a wide array of entities providing electric and natural gas services in Indiana. Walt Grudzinski who serves on the Energy Committee and the Workforce Development Committee will serve as the key contact point for questions and further input which Workforce Development may require from the Energy Committee. In addition, the Committee has determined that Mark Maassel should be the back-up contact point for questions and further input as needed by the Workforce Development Committee. He will engage the appropriate resources to support the Workforce Development Committee

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
Minimal	Minimal	Supervisory experience which informs the individual on the training required to function in cybersecurity roles inside the energy industry.	Existing payroll of Energy Committee Members	N/A	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. This will provide a skilled pool of applicants ready to address cybersecurity issues from which the energy industry can draw to staff our workforce.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Better skilled employees reduce the risk of mistakes and oversights as we strive to protect utility operating systems or to recover should an incident occur. The Workforce Development Committee is likely a better source to assess the cost of developing the needed programs here in Indiana.

19. What is the risk or cost of not completing this deliverable?

a. Most likely the industry will hire individuals from outside of Indiana. It will be a missed opportunity for Hoosiers to learn and develop the skills needed.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The Energy Committee believes these are better developed by the Workforce Development Committee. For us, success is simply having Hoosiers who possess the skills the energy industry needs as we look to fill openings in our staff.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. Virginia has a program which warrants review by the IECC.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. Any state other than those listed in response to question 21 may be a potential control.

Other Implementation Factors

---

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable**?

a. None

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. The Workforce Development Committee is best suited to address this issue.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. In responses to the questions asked in Phase 1, we have alerted the Workforce Development Committee of our needs.

27. Can this deliverable be used by other sectors?

a. Yes
b. We believe that all sectors will benefit from enhanced training in the skills needed for cybersecurity.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All committees and working groups could benefit from this deliverable.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Others are better positioned and informed to address this issue. However, it would seem to be a wonderful opportunity to highlight the capabilities of Indiana's educational system and the ability to "tune" that system to train individuals in a new, developing set of skills needed in the workplace.
b. Just to reiterate, the IECC Energy Committee recognizes that we will need to engage in an ongoing, bi-directional dialog with the Workforce Development Committee and others to assure that the appropriate training and education is being provided to those entering the field. This will be critical given the rapidly changing cyber environment and the need for flexibility and adaptability to meet the challenges and seize the opportunities presented by these changes.

Evaluation Methodology

Objective 1: IECC Energy Committee will provide the IECC Workforce Development Committee the needs of the energy sector, as well as examples to consider as Indiana cybersecurity training and apprenticeship programs, are being developed by July 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Contacts

Deliverable: Contacts

General Information

1. **What is the deliverable?**
   a. Identify energy companies within the State of Indiana, form of ownership and how cyber is managed. Develop and maintain a critical contact database.

2. **What is the status of this deliverable?**
   a. 100% complete

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable**?
   a. Appropriate contact information is available in the event of a cyberattack.

6. **What metric or measurement will be used to define success?**
   a. This will be measured by the existence of a contact list and its updating. The updates will be done by the IURC. The survey will be used to verify, among other things, contact information.

7. **What year will the deliverable be completed?**
   a. 2018
   b. An initial list will be developed in 2018. However, this will need periodic updating and will never be finished.

8. **Who or what entities will benefit from the deliverable?**
    a. All individuals and organizations who are a part of the protection against cyberattacks or in recovering from cyberattacks.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. We are not aware of any overlap on this issue.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. We believe that this deliverable does not require input from other IECC Committees and/or Working Groups.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. The IURC will be the central point for the collection of the information. The IURC and the IDHS will be involved since they will be the central points in a cyber emergency.

12. **Who should be main lead of this deliverable?**
    a. The IURC leads the effort to assemble the contact information. In addition, the Energy Committee is structured so that information flows to Mark Maassel at the Indiana Energy Association. It is his responsibility to share the information with the Energy Committee and to provide feedback to others.

13. **What are the expected challenges to completing this deliverable?**
    a. We do not anticipate major challenges to completing this deliverable.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
On a routine basis, survey the Indiana energy utilities to determine the appropriate contacts for cyber issues.	The Indiana Utility Regulatory Commission already gathers critical contact information for physical events which impact the operations of electric and natural gas utilities. They will expand this information gathering and updating to include cyber contacts.	Completed	June 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
Less than 1	Less than 1		Cost will be covered by each respondent and the IURC	None	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Assure the existence of up-to-date contact information.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Up-to-date contact information will assist in more timely and responsive communications planning, testing and recovery.

19. What is the risk or cost of not completing this deliverable?

a. Less than ideal exchange of information and ideas in planning, testing and recovery.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Responses to the request for up-to-date contact information will define success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Most other states collect this type of information.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. The Energy Committee is unaware of any state that does not gather such information.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Needed personnel and other resources are in place.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Committee discussions have identified the IURC as the best-positioned entity to gather the needed information.

27. Can this deliverable be used by other sectors?

a. Yes
b. This approach could work for any sector which might be planning for, testing or involved in recovery from a cyber incident would benefit. Other approaches might work for them as well. We selected this approach as a practical and effective mechanism in the energy industry.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Both the IURC and IDHS will need and want this information. This follows the existing practices for the IDHS Emergency Operations Center and will simply be expanded to include both contacts for physical interruptions of service as well as cyber interruptions.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No

30. What are other public relations and/or marketing considerations to be noted?

a. While others are much better positioned and informed to answer this question, we do not necessarily see this item as a key for either public relations or marketing consideration.

Evaluation Methodology

Objective 1: Over eighty-five percent of Indiana electric and natural gas utilities provided the Indiana Utility Regulatory Commission's Emergency Support Function lead on behalf of Indiana Department of Homeland Security a cybersecurity contact by June 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: The Indiana Utility Regulatory Commission's Emergency Support Function lead will maintain the cyber contact list on behalf of the Indiana Department of Homeland Security Emergency Operations Center annually.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis – Year 2
☐ Quantifiable Measurement
☐ Other

Deliverable: Coordinate with Others

Deliverable: Coordinate with Others

General Information

1. **What is the deliverable?**
   a. Coordinate with Working Groups as appropriate.

2. **What is the status of this deliverable?**
   a. While the work of coordinating with others will be an ongoing process, for the first year the Energy Committee has completed this deliverable.

3. **Which of the following IECC goals does this deliverable meet?**

☐ Establish an effective governing structure and strategic direction.
☒ Formalize strategic cybersecurity partnerships across the public and private sectors.
☐ Strengthen best practices to protect information technology infrastructure.
☐ Build and maintain robust statewide cyber-incident response capabilities.
☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**

☐ Research – Surveys, Datasets, Whitepapers, etc.
☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. We have supported the work of other sectors as well as achieved an appropriate level of sharing of information and risks through existing channels such as the E-ISAC. The Energy Sector will continue to share information through these types of channels. From there, information should be shared through a Multi-sector ISAC.

6. **What metric or measurement will be used to define success?**
    a. Because energy sector companies already follow the rules and guidelines established by the NERC and TSA, the sector has strong cyber plans and processes in place. The Indiana Energy Association (IEA) will conduct an annual survey of the energy sector asking questions to measure the status of cyber preparedness. They are:
        i. Do you have a plan?
        ii. If so, do you review and exercise the plan periodically?

7. **What year will the deliverable be completed?**
    a. 2018. The survey was conducted in May and June. Final results were sent to the IECC on June 2018. The results are also attached as Supporting Documentation.
    b. The IECC final report will serve as the completion of this deliverable.

8. **Who or what entities will benefit from the deliverable?**
    a. Done correctly, all participants will benefit.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. We are not aware of an overlap at the moment; however, recognize that the potential for overlap grows as both federal and state government move ahead with various initiatives

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. We believe that cybersecurity is best advanced by using the existing infrastructure. Specifically, each sector should continue to work with their ISAC who in turn should work with the multi-sector ISAC. State of Indiana contacts should be coordinated through IDHS. IDHS can work with the IURC for energy sector contacts.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Our experience with Subsector Coordinating Councils has been positive. The entities who make up these Councils are the individuals and organizations who need to be involved. From the standpoint of other sectors (e.g., the Financial Sector) we are hopeful that the correct individuals and organizations are engaged. Thus, the issue is more about opening lines of communications between the Councils. Furthermore, state-based associations like the IEA will be available to IDHS.

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Mark Maassel at the IEA. It is his responsibility to share the information with the Energy Committee and to provide feedback to others

13. What are the expected challenges to completing this deliverable?

a. We are not aware of any challenges at this point.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability**?

a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Support others as appropriate	Energy Committee	100%	May 2018	
Respond to questions asked by other Committees & Working Groups	Energy Committee	100%	November 2017	
Provide appropriate information to the Energy ISAC. We hope to receive information which we can act upon from other ISAC's through a cross-sector ISAC.	Energy Committee	100% though ongoing. This is built into our existing processes.	May 2018	
Provide a contact to Chetrice Mosely for an individual at the North American Electric Reliability Council so she can assess whether such a speaker should present to the IECC or at the Cyber Summit.	Stan Partlow	100%	June 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
No additional staff is required.					

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. The development of a cohesive cyber plan for Indiana which does not create unwarranted requirements on time or funds which do not enhance cybersecurity and preparedness.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Better coordination of efforts and of information exchanges will reduce cybersecurity risk and impact. The costs are all a part of the existing business costs for the energy utility industry.

19. What is the risk or cost of not completing this deliverable?

a. A less cohesive cyber plan for Indiana.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success will be shown by working with other Committees and Working Groups effectively.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No, we are not aware of any.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No, we are not aware of any.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. We are not aware of any.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Ongoing communications designed to enhance cybersecurity are welcome.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. We have, through the questionnaire completed in November 2017, reached out to several committees and responded to their questions.

27. Can this deliverable be used by other sectors?

a. Yes
b. We would assume that all Committees and Working Groups are supportive of communicating to enhance cybersecurity in Indiana.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All stakeholders can be informed that the energy utility industry and this Committee are willing to work with others to support enhancing cybersecurity in Indiana.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes, assuming that there are no confidentiality or security concerns with the information.

30. What are other public relations and/or marketing considerations to be noted?

a. While others are much better positioned and informed to answer this question, we do not necessarily see this item as a key for either public relations or marketing consideration.

Evaluation Methodology

Objective 1: IECC Energy Committee will coordinate with other committees and working groups as needed to effectively complete the State Cybersecurity Strategic Plan by September 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Energy Committee will share information with Energy ISAC regarding Indiana's new cyber sharing resources by December 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Metrics

Deliverable: Metrics

General Information

1. **What is the deliverable?**
    a. Establish metrics to assess the overall risk to the State of Indiana regarding Energy utility operations.

2. **What is the status of this deliverable?**
    a. 100% Complete.

3. **Which of the following IECC goals does this deliverable meet?**

☒ Establish an effective governing structure and strategic direction.
☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
☐ Strengthen best practices to protect information technology infrastructure.
☐ Build and maintain robust statewide cyber-incident response capabilities.
☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**

☐ Research – Surveys, Datasets, Whitepapers, etc.
☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The goal is to establish accountability and clarity of the effectiveness of cybersecurity programs and response plans. Energy sector companies already follow the rules and guidelines established by NERC and TSA, the sector has strong cyber plans and processes in place. The IEA will conduct an annual survey of the energy sector asking questions to measure the status of cyber preparedness. They are:
        i. Do you have a plan?
        ii. If so, do you review and exercise the plan periodically?

6. **What metric or measurement will be used to define success?**
    a. Metrics are in place inside the energy industry with which the companies comply. As Indiana develops its metrics, we will seek to dovetail existing metrics used in the energy industry into the Indiana framework without creating unnecessary work. This has been accomplished with the creation of the survey described in Question 5.

7. **What year will the deliverable be completed?**
    a. 2018
    b. Indiana's electric and natural gas energy industry responded to the survey which was developed to assure that effective cybersecurity planning is in place in the energy industry and help to advance cybersecurity.

8. **Who or what entities will benefit from the deliverable?**
    a. Generally speaking, metrics provide valuable insights into planning and execution of the measures taken to address cyber risks.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. We do not believe there is any overlap at the moment. The risk will be that the Indiana specific metrics do not recognize the existing federal requirements creating added work which might detract from addressing cyber issues.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Coordination with the Strategic Resource Task Force will be important.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. This work will largely flow from the ongoing engagement with federal agencies. Key among these are DHS, TSA, FERC and NERC.

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Mark Maassel at the IEA. It is his responsibility to share the information with the Energy Committee and to provide feedback to others

13. **What are the expected challenges to completing this deliverable?**
    a. Assuring adequate flow of information to other committees/task forces and a similar flow from them to the Energy Committee.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
The IECC Energy Committee developed a set of two questions which can be asked annually to assess planning, preparedness and recovery in the utility energy industry.	This will be coordinated by the IEA and provided to the IECC.	100%	June 2018	Given the pervasive nature of federal requirements, relatively few questions and one metric are needed to assess the status of the energy industry in Indiana.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
No additional staff is required.					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Though pervasive federal regulation and guidance of cyber issues exists in the energy utility arena, this will provide a metric to quickly and effectively relay the status to Indiana stakeholders.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. The metric will quickly identify the situation here in Indiana. It should be noted that a reduction in cyber risk is already achieved through the federal regulation and guidance which is in place. This metric will help in communicating a complex set of rules and their application in a highly specialized, technical industry to those in Indiana who seek to understand the status of this industry.

19. What is the risk or cost of not completing this deliverable?

a. The vast majority of cybersecurity in the energy utility industry results from existing federal regulations and guidance.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Responsiveness of energy utility industry participants will be a measure of success. The baseline was established when the first ever survey was sent to the industry. One hundred percent of those surveyed responded to the survey providing a comprehensive look at the planning that exists within the Indiana energy utility space.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. We are not aware of any.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. We are not aware of any.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. We are not aware of any.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. See the "Owner" column in the "Tactic Timeline" table above.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. This was developed by the Energy Committee.

27. Can this deliverable be used by other sectors?

a. Yes
b. This may be applicable to and useful for other sectors. However, the metric was developed with an eye to the existing regulations and guidelines which the energy utility industry follows. We believe that the level of existing regulation and guidelines are unique to this industry.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. The Indiana Executive Cybersecurity Council. The results of the survey are attached as a part of the Supporting Documentation.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. While others are much better positioned and informed to answer this question, we do not necessarily see this item as a key for either public relations or marketing consideration.

Evaluation Methodology

Objective 1: IECC Energy Committee will provide the utility energy industry an annual survey that will assess cybersecurity planning, preparedness and recovery posture by June 2018. A summary of the results from all those who were surveyed was sent to the IECC.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Eighty percent of all utilities will complete annual survey by July 2018. The actual result was one hundred percent participation with all responses received prior to June 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- American Public Power Association (APPA) – Cybersecurity and the Electric Sector
- Electricity Subsector Coordinating Council (ESCC) Brochure
- Federal Energy Regulatory Commission (FERC) Critical Energy/Electric Infrastructure Information (CEII) Regulations
- IECC Energy Committee Annual Metrics Report
- IECC Energy Committee Commonwealth of Virginia (CoV) Briefing
- National Conference of State Legislatures (NCSL) – State Efforts to Protect the Electric Grid

American Public Power Association (APPA)

Cybersecurity and the Electric Sector

June 2017

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

ISSUE BRIEF June 2017

Cybersecurity and the Electric Sector

Summary

The electric utility industry (including public power utilities) takes very seriously its responsibility to maintain a strong electric grid and it is the only critical infrastructure sector besides nuclear power that has any mandatory and enforceable federal regulatory standards in place for cybersecurity. As the grid evolves, unfortunately, so do threats to its integrity. The threat of cyber-attacks is relatively new compared to long-known physical threats, but an attack with operational consequences could occur and cause disruptions in the flow of power if malicious actors are able to hack into data overlays used in some electric generation and transmission infrastructure. Furthermore, such an attack could also cause public power utilities to incur liability for damages. While the American Public Power Association (Association or APPA) believes that the industry itself, with the North American Electric Reliability Corporation (NERC), has made great strides in addressing cybersecurity threats, vulnerabilities, and potential emergencies, it recognizes that emergency situations warranting federal involvement may arise.

Background and Congressional Action

The electric utility sector is the only critical infrastructure sector besides nuclear power plants (a part of the overall sector) that has any mandatory and enforceable federal regulatory regime in place for cybersecurity. Congress approved the standards regime for the bulk power system in the Energy Policy Act of 2005 (Section 215 of the Federal Power Act). Under Section 215, NERC, working with electric industry experts, regional entities, and government representatives, drafts reliability and cybersecurity standards that apply across the North American grid, inclusive of Canada. Participation by industry experts and compliance personnel in the NERC standards development process ensures that the standards are technically sound, fair, and balanced. The Federal Energy Regulatory Commission (FERC) has the power to then approve or remand those standards as they apply in the United States. To ensure compliance, NERC conducts rigorous audits and can levy substantial fines for non-compliance. Additionally, FERC can instruct NERC to develop new or revised reliability standards with a very short turn-around time.

To date, the electric utility sector's Federal Power Act (FPA) Section 215 processes and its actions beyond the Section 215 regime have prevented a successful cyber-attack causing operational consequences on the bulk electric system in the United States. That said, APPA has long recognized that increased information sharing and appropriately tailored liability protection would further enhance the industry's ability to guard against cyber-attacks. As such, the Association strongly supported passage of the Cybersecurity Act of 2015, which was incorporated as Division N of H.R. 2029, the Consolidated Appropriations Act, 2016. The Act set up policies and procedures for sharing cybersecurity threat information between the federal government and private entities (which include public power) and between private entities and provides limited liability protection for these activities if conducted in accordance with the Act.

In addition to the Cybersecurity Act of 2015, the Association strongly supported Section 61003 of P.L. 114-94 (the "FAST Act"), which gave the Secretary of Energy broader authority to address grid security emergencies under the FPA and clarified the ability of FERC and other federal agencies to protect sensitive Critical Electric Infrastructure Information (CEII) from public disclosure under the Freedom of Information Act (FOIA) and other sunshine laws. Specifically, the provision directed that FERC-designated CEII be exempt from disclosure for a period of up to five years with a process to lift the designation or challenge it in court and established sanctions for the unauthorized disclosure of shared information. FERC issued a final rule to implement this provision on December 21, 2016.

Outside of the legislative process, the Association and its members, as well as other utilities, continue to participate in the NERC Critical Infrastructure Protection (CIP) standards drafting process on cyber and physical security. (See APPA's "Physical Security and the Electric Sector" issue brief for more information on the physical-security standard.) As attacks on critical electric infrastructure are ever-changing, so must be the nature of our defenses, whether they are designed to protect cyber or

physical assets. As such, CIP Version 5 are in effect and became enforceable on July 1, 2016.

APPA is also involved with internal and external working groups to enhance the security of the electric grid. The Association and its members play a leadership role in the Electricity Subsector Coordinating Council (ESCC), the government/industry partnership focused on security and information sharing that is mentioned earlier in this document. Through the ESCC, APPA works with the other critical infrastructure sectors, such as the downstream natural gas and dam sectors.

Administrative Action

On May 11, 2017, President Trump signed a long-anticipated Executive Order (EO), "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The EO states that "It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure." It directs the Department of Energy (DOE), Department of Homeland Security, and Director of National Intelligence, along with other stakeholders, to assess within 90 days: "(i) the potential scope and duration of a prolonged power outage associated with a significant cyber incident against the United States electric subsector; (ii) the readiness of the United States to manage the consequences of such an incident; and (iii) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident." APPA is still reviewing the EO and will provide additional analysis as necessary. President Trump's EO builds on the one issued by former President Obama in February 2013 requiring the creation of a cybersecurity framework, which was subsequently released by the National Institute for Science and Technology (NIST) in February 2014. The Association has strongly encouraged its members to adopt this framework and evaluate their cybersecurity plans.

Finally, the Association has also partnered directly with DOE. APPA and DOE signed a three-year Cooperative Agreement in 2016 for up to $2.5 million per year to accelerate the Association's efforts to help its members understand and implement resiliency, cybersecurity, and cyber-physical solutions, including refining and improving the adoption of advanced control concepts. We respectfully encourage Congress to continue fully funding research in this area through DOE's Office of Electricity Delivery and Energy Reliability (OEDER).

American Public Power Association Position

Protecting the cybersecurity of the electric grid is of upmost importance to public power utilities and the electric utility industry as a whole. The regulations and standards ("NERC-FERC") process set up in the 2005 Energy Policy Act continue to provide a solid foundation for strengthening the industry's security posture. These mandatory standards evolve with input from subject-matter experts from across industry and government. However, we recognize that we cannot protect all assets from all threats all the time, and instead must manage risk. APPA believes that close coordination among industry and government partners at all levels is imperative to deterring attacks and preparing for emergency situations and, as such, will continue to invest considerable resources into this effort.

American Public Power Association Contacts

Amy Thomas, Government Relations Director, 202-467-2934 / athomas@publicpower.org

Cory Toth, Government Relations Director, 202-467-2939 / ctoth@publicpower.org

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. We represent public power before the federal government to protect the interests of the more than 49 million people that public power utilities serve, and the 93,000 people they employ. Our association advocates and advises on electricity policy, technology, trends, training, and operations. Our members strengthen their communities by providing superior service, engaging citizens, and instilling pride in community-owned power.

Electricity Subsector Coordinating Council (ESCC)

Brochure

November 2017

NOVEMBER 2017

ESCC

Electricity Subsector Coordinating Council

Protecting the energy grid from threats that could impact national security is a responsibility shared by both the government and the electric power sector.

The Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the federal government and the electric power industry, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC includes electric company CEOs and trade association leaders representing all segments of the industry. Its counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

Background

In October 2010, the National Infrastructure Advisory Council (NIAC) issued a report, *A Framework for Establishing Critical Infrastructure Resilience Goals*, that included nine recommendations. The first recommendation was:

> **NIAC Recommendation:** "The White House [will] initiate an executive-level dialogue with electric and nuclear sector CEOs on the respective roles and responsibilities of the private sector in addressing high-impact infrastructure risks and potential threats... ."

This recommendation was the impetus for initial meetings in July 2012 between an ad hoc group of industry CEOs and Department of Energy (DOE) Secretary Steven Chu and Department of Homeland Security (DHS) Secretary Janet Napolitano. These meetings resulted in a classified briefing for the industry in September 2012 and led to the formation of the Joint Electric Executive Committee, which was convened in January 2013 and which had a commitment to meet quarterly with the Deputy Secretaries of DOE and DHS.

Ultimately, the Joint Electric Executive Committee transitioned to its current official role as the ESCC.

ESCC Areas of Focus

Industry and government leaders have agreed to focus on four main areas that improve the security posture of the industry and the nation. To support the deployment of tools, improve the flow of threat information, prepare for incidents, and work closely with other interdependent infrastructure sectors, the ESCC has organized into strategic committees with the following missions:

Threat Information Sharing: Improve and institutionalize the flow of, and access to, actionable information among public- and private-sector stakeholders.

Industry-Government Coordination: Establish unity of effort and unity of messaging between industry and government partners to support the missions of the ESCC both during crises and in steady state.

Research & Development: Coordinate government and industry efforts on strategic infrastructure investments and R&D for resilience and national security-related products and processes.

Cross-Sector Liaisons: Develop strong partnerships at all levels of the Electricity, Communications (Telecommunications), Oil and Natural Gas (Downstream Gas), Financial Services, Transportation Systems, and Water and Wastewater Systems (Water) sectors to plan and respond to major incidents, to better understand and protect our mutual dependencies, and to share information effectively and efficiently to improve cross-sector situational awareness.

Security Executive Working Group

To support the mission of the ESCC, a Security Executive Working Group (SEWG) convenes by phone on a monthly basis and creates ad hoc teams to accomplish the goals identified by the CEOs and Deputy Secretaries. In parallel to this effort, the government also has organized around these goals with a commitment to align government and industry efforts.

ESCC Official Roster

November 2017

Leadership (3)

Tom Fanning, Southern Company (co-chair)
Kevin Wailes, Lincoln Electric System (co-chair)
Duane Highley, Arkansas Electric Cooperative (co-chair)

Steering Committee (9)

Sue Kelly, American Public Power Association
Sergio Marchi, Canadian Electricity Association
Tom Kuhn, Edison Electric Institute
John Shelk, Electric Power Supply Association
Andrew Ott, PJM (representing the ISO/RTO Council)
Mike Wallace, National Infrastructure Advisory Council
Jim Matheson, National Rural Electric Cooperative Association
Gerry Cauley, North American Electric Reliability Corporation
Maria Korsnick, Nuclear Energy Institute

Asset Owners
(19: 13 investor-owned electric companies; 3 electric cooperatives; 3 municipal electric companies)

Nick Akins, American Electric Power
Jim Torgerson, Avangrid
Scott Miller, City Utilities of Springfield
John McAvoy, Consolidated Edison
Tom Farrell, Dominion
Lynn Good, Duke Energy
Pedro Pizarro, Edison International
Gianna Manes, ENMAX Corporation
Chris Crane, Exelon Corporation
Greg Ford, Georgia System Operations Corporation
David Saggau, Great River Energy
Connie Lau, Hawaiian Electric Industries
William Fehrman, MidAmerican Energy Co.
John Bilda, Norwich Public Utilities
Jack Reasor, Old Dominion Electric Cooperative
Tony Earley, PG&E Corporation
Bill Spence, PPL Corporation
Gil Quiniones, New York Power Authority
Ben Fowke, Xcel Energy

ESCC Coordination

Coordination among senior government and industry executives helps to ensure an effective response, appropriate prioritization and allocation of resources, and support for deviation from standard procedures during an incident.

ESCC Stakeholders

Government

- Federal Agencies
- Regulators
- PMAs
- Law Enforcement
- State, Local, Tribal, & Territorial
- Canadian Agencies & Provinces

Industry

- Electric Companies
- Trade Associations
- ISOs & RTOs
- NERC
- E-ISAC
- Canadian Electric Companies

External Groups

- Other Critical Sectors
- Vendors
- Critical Customers
- Media

Coordination

- Security to support restoration
- Media and public affairs messaging
- Logistical support, staging

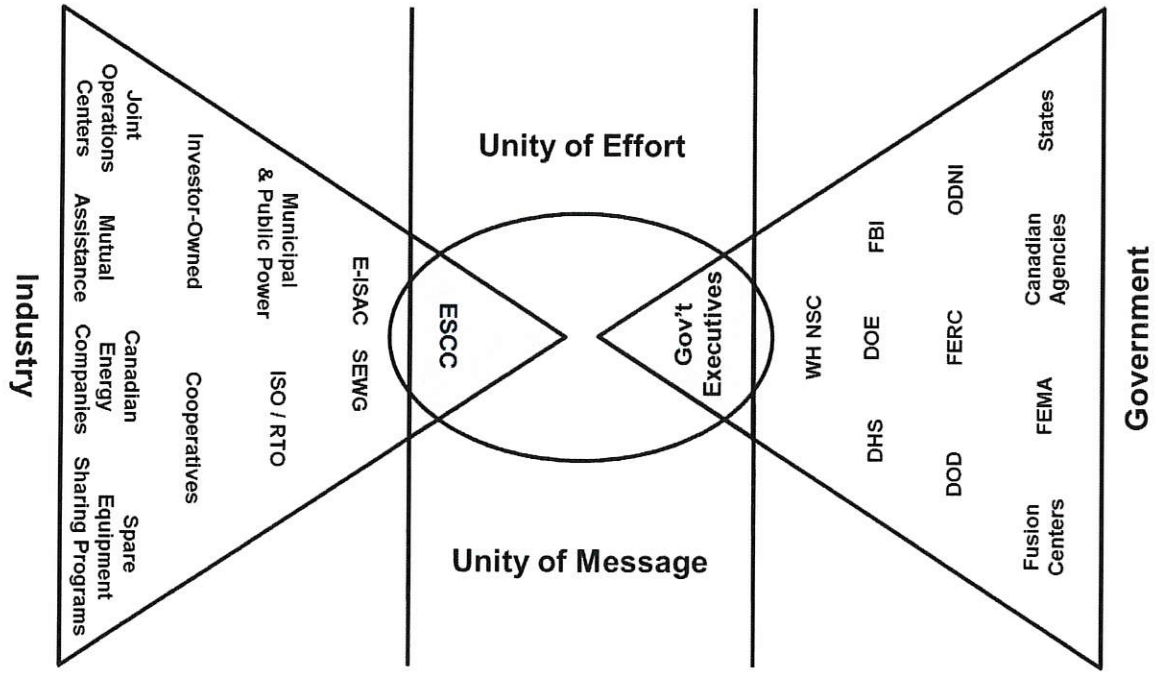
Resource Allocation

- Equipment, hardware, and materials
- Human resources and expertise

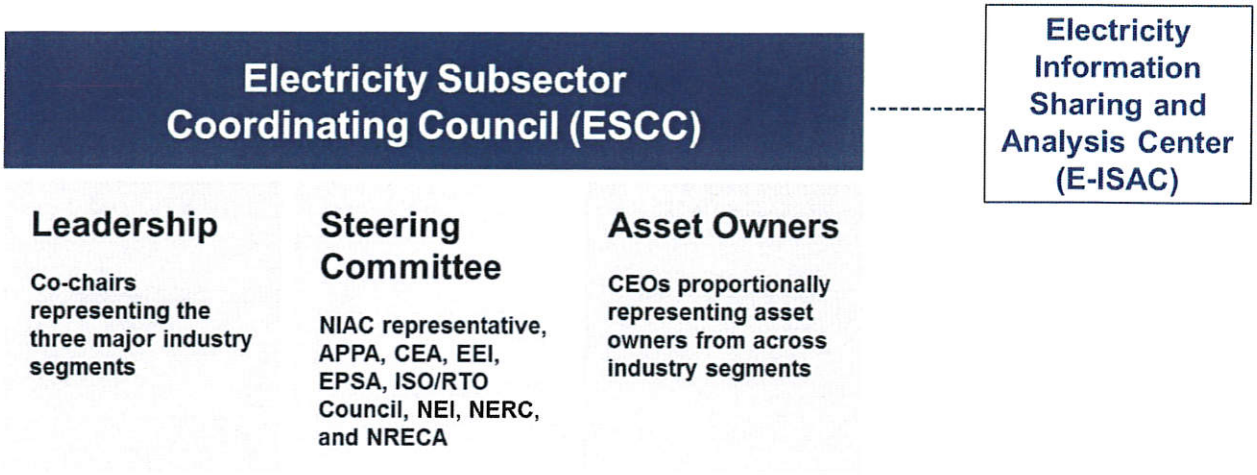
Conflict Resolution

- Investigation versus restoration
- Prioritization of recovery
- Distribution of limited resources

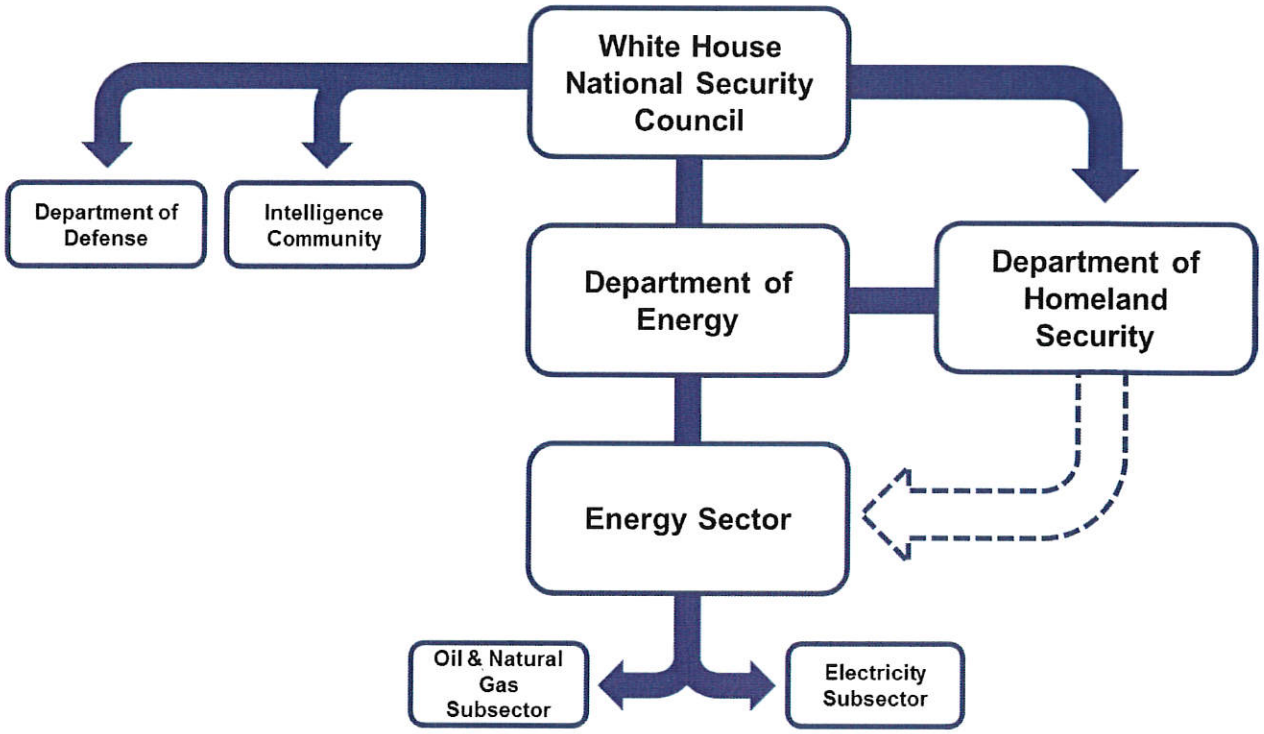
Industry-Government Coordination



ESCC Member Structure



Energy Sector-Government Organizational Structure



ESCC
Electricity Subsector Coordinating Council

Federal Energy Regulatory Commission (FERC)

Critical Energy/Electric Infrastructure Information (CEII) Regulations

November 2016

FERC Federal Energy Regulatory Commission

Critical Energy/Electric Infrastructure Information (CEII) Regulations

The Commission has established procedures for gaining access to critical energy/electric infrastructure information (CEII) that would otherwise not be available under the Freedom of Information Act (FOIA):

- CEII is defined as infrastructure explicitly covers proposed facilities, and does not distinguish among projects or portions of projects.
- These procedures details which location information is excluded from the definition of CEII and which is included.
- The rule addresses some issues that are specific to state agencies, and clarifies that energy market consultants should be able to get access to the CEII they need.
- The rule modifies the proposed CEII process and delegates' responsibility to the CEII Coordinator to process requests for CEII and to determine what information qualifies as CEII.

Order No. 833 PDF, issued November 17, 2016
The FAST Act, signed into law by President Barack Obama in December 2015, adds section 215A to the Federal Power Act to improve security and resilience of energy infrastructure in the face of emergencies. The FAST Act required FERC to issue regulations aimed at securing and sharing CEII. Specifically, the Order includes the following amendments to the CEII regulations:

- Establishes criteria and procedures to designate information as CEII;
- Prohibits unauthorized disclosure of CEII;
- Establishes sanctions for FERC employees and certain other individuals who knowingly and willfully make unauthorized disclosures; and
- Facilitates voluntary sharing of CEII among federal, state, political subdivision and tribal authorities; the Electric Reliability Organization; regional entities; owners, operators and users of critical electric infrastructure; and other entities deemed appropriate by the Commission.

Order No. 702 PDF, issued October 30, 2007- This Order:

- Modifies non-disclosure agreements and modifies the Commission's process to allow the CEII Coordinator to respond to CEII requests by letter.
- This rule provides landowners access to alignment sheets for the routes across or in the vicinity of their properties.
- This rule includes a provision for assessing fees for requests.
- This rule limits the portions of forms and reports the Commission defines as containing CEII.
- The rule eliminates as a category of documents the Non-Internet Public designation.
- The rule provides that the Commission will seek a requester's date and place of birth on a case-by-case basis rather than require that information with every request for CEII and the request for social security numbers is being eliminated.

Order No. 683 PDF, issued September 21, 2006 - This Order:

- Clarifies CEII as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure;
- Details which location information is excluded from the definition of CEII and which is included; and
- Modifies the CEII process by requiring requesters to submit an executed non-disclosure agreement with their requests.
  - General Non-Disclosure Agreement PDF
  - Media Non-Disclosure Agreement PDF
  - Federal Agency Acknowledgement and Agreement PDF

Order No. 662 PDF, issued June 21, 2005 - This Order:

- Removes federal agency requesters from the sope of the rule;
- Modifies the application of non-Internet public (NIP) treatment; and
- Clarifies obligations of requesters.

Order No. 649 PDF, issued August 3, 2004 - This Order:

- Primarily eases the burden on owners/operators of energy facilities that are seeking CEII relating to the their own facility, and
- Simplifies federal agencies' access to CEII.

These changes will facilitate legitimate access to CEII without increasing vulnerability of the energy infrastructure.

Order No. 643 PDF, issued July 23, 2003
This Order requires companies to make information directly available to the public under certain circumstances.

Order No. 630-A PDF, issued July 23, 2003
The Commission amended Order No. 630:

- To increase the numbers of copies filed;
- Clarified the filing process for submitting CEII; and
- The instructions for requesting rehearing of the CEII Coordinator's decision

Order No. 630 PDF, issued February 21, 2003- This Order:

- Adopts the definition of critical infrastructure that explicitly covers proposed facilities;
- Does not distinguish among projects or portions of projects;
- Details which location information is excluded from the definition of CEII and which is included;
- Addresses some issues that are specific to state agencies;
- Clarifies that energy market consultants should be able to get access to the CEII they need; and
- Adopts a CEII process and delegates responsibility to the CEII Coordinator to process requests for CEII and to determine what information qualifies as CEII.

IECC Energy Committee
Annual Metrics Report

June 2018

Indiana Executive Cybersecurity Council

Energy Committee

Annual Update and Measurement of Metrics

2018

Company	Do you have a plan?	Do you review and exercise the plan periodically?
Citizens Energy Group	Yes	Yes
Duke Energy	Yes	Yes
Hoosier Energy	Yes	Yes
IMPA	Yes	Yes
IN MI Power/AEP	Yes	Yes
IPL/AES	Yes	Yes
MISO	Yes	Yes
NIPSCO	Yes	Yes
Vectren	Yes	Yes
WVPA	Yes	Yes

IECC Energy Committee

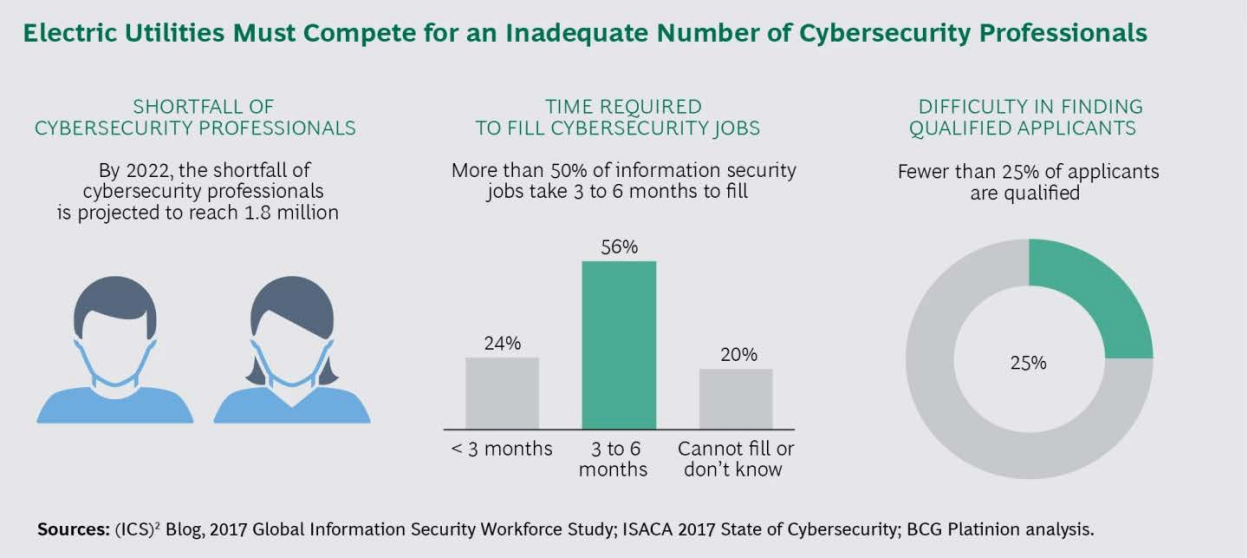
Commonwealth of Virginia (CoV) Briefing

May 2018

TO: Mark Maassel, Indiana Energy Association President
CC: Energy Working Group, Indiana Executive Council on Cybersecurity
FROM: Jennifer de Medeiros, Infrastructure Security Analyst, AES Corp.
RE: Cyber Workforce Training Standards & Standardbearers

Given the pace of technological change and rapidly sophisticating threat landscape, the State of Indiana is challenged to grow and retain a skilled workforce that can continuously evolve alongside the cyber ecosystem. The Commonwealth of Virginia is regarded as having set the standard for a diversified training portfolio that targets a cross-section of residents, including traditionally underserved populations. It is recommended that the IECC consider similar avenues that can offer targeted training opportunities for strongly needed professional functions within the critical infrastructure sectors.

This is especially important for the energy industry, which has a unique need for not only information technology (IT) and operations technology (OT) professionals, but professionals who can navigate both systems. Given the complexity of securing both IT and OT systems, utilities in particular suffer from a shortage of professionals who can address cybersecurity needs. Teaching IT professionals about OT—and OT professionals about IT—is not always easy or effective. Education and training organizations should continue to focus on developing converged IT-OT cybersecurity practitioners using a variety of methods.



Indiana should support cyber programs at community colleges, and support accreditation as National Centers of Academic Excellence. Indiana is well known for its excellent higher education cyber programs at Purdue, Indiana University, IUPUI and others. However, these programs may be outside the reach of many Hoosiers due to their cost and length. In Virginia, there are 62 Centers of Excellence, 5 of which are 2-year community colleges. Offering more options – including converged IT-OT training options – for Hoosiers of all income levels will ensure cybersecurity is sewn into the fabric of our education system.

Apprenticeship programs are a proven method for filling talent gaps and accelerating learning – without the cost of formal education. Because there are so few formal educational opportunities for the IT-OT system, utilities and energy partners must offer hands-on, tacit learning experiences to train their own personnel and facilitate knowledge transfer within the industry. It is not easy to educate IT professionals in an OT environment, and vice versa. Cybersecurity apprenticeships can be particularly effective in

navigating in this unique environment, which typically has a technological “reset” of seven years. Apprentice programs also accelerate learning without the cost of long-term formal education programs.

- https://www.dol.gov/apprenticeship/industry/energy.htm

Veterans who have served and protected the Nation are well-positioned to transition into much needed cybersecurity jobs. Veteran job seekers are more likely than non-veterans to be underemployed, despite the fact that the majority of employers report that they perform "better than" or "much better than" non-veterans. CyberVirginia has launched a Cyber Veterans Initiative that aims to provide training programs, apprenticeships, and employment to veterans of all skill levels, ensuring the programs are accessible in terms of cost and time. Pursuing a similar veterans initiative here in Indiana can similarly dovetail with the critical need for IT/OT professionals, and ensure Indiana is seen as a forward-thinking, economically productive state for a variety of cyber careers.

National Conference of State Legislatures (NCSL)

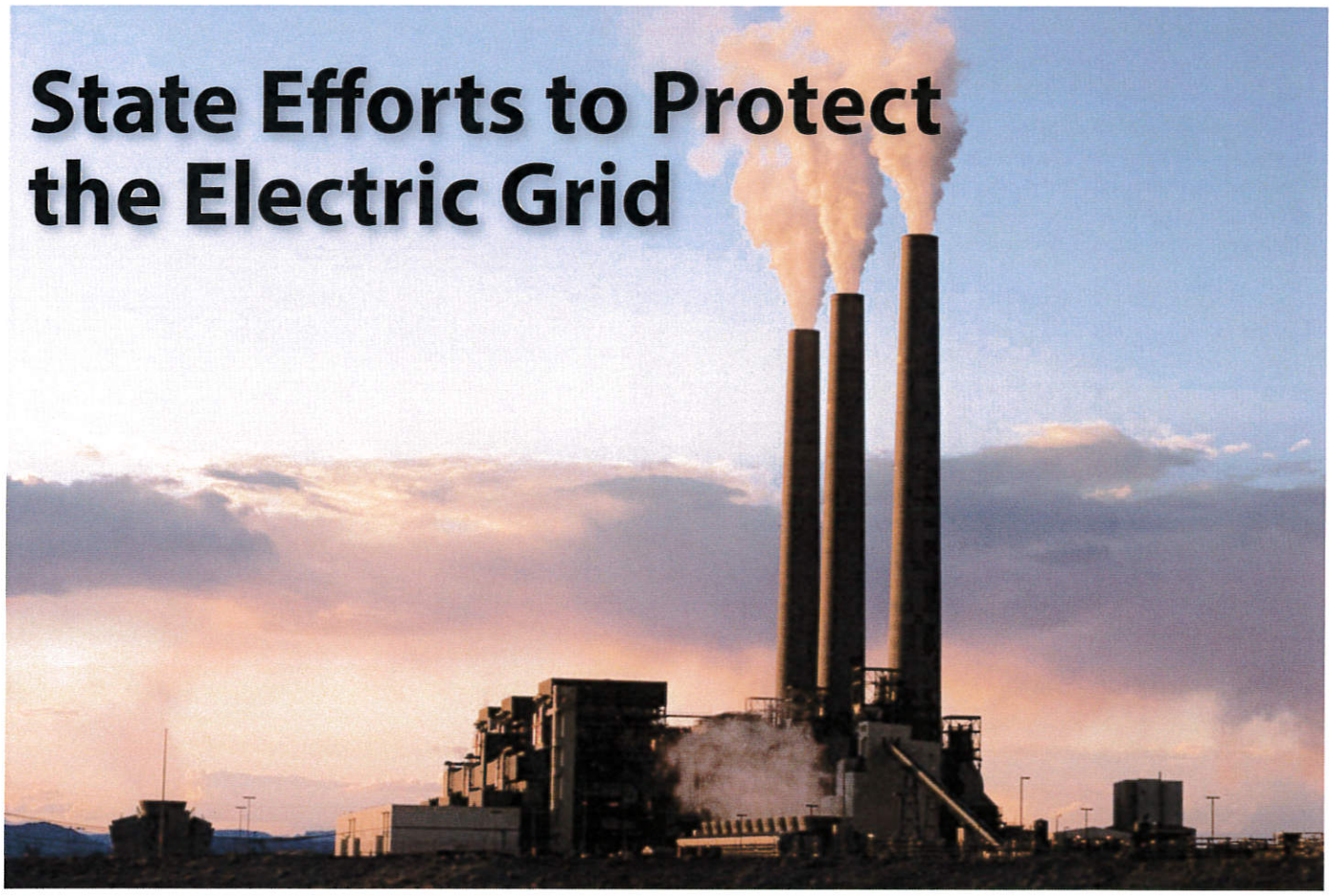
State Efforts to Protect the Electric Grid

April 2016

NCSL

Strong States, Strong Nation

State Efforts to Protect the Electric Grid



BY DANIEL SHEA

April 2016

Overview

There are growing threats to the nation's critical infrastructure and state legislatures have been working diligently to address these issues through a variety of measures. Recent events have highlighted weaknesses in the nation's aging electrical grid, sections of which originated more than a century ago.[1] Even as Superstorm Sandy and Hurricane Irene continue to loom large in the collective memory, Hurricane Joaquin ushered in October 2015 by battering the Eastern seaboard with record levels of rain and 100-mph winds. The increased intensity of recent weather events is raising awareness about the physical threats to the grid. At the same time, a growing array of cyberthreats to energy infrastructure have led experts to increasingly draw attention to the grid's technological vulnerabilities.

Some legislators have sought to make the grid more resilient by diversifying energy production. More than a dozen states introduced legislation in 2015 that calls for greater diversity in power sources—from expanding renewables to supporting nuclear and fossil fuels. At the same time, there has been a significant push to encourage and incorporate microgrids into the electrical system. These standalone systems can operate independently and supply power to a specific area in the event of a broader disruption to the electric system. Some lawmakers are eager to promote microgrids, given the economic impacts of widespread power outages. It has been estimated that a single day without power in New York City would cost $1 billion.[2]

Many states are also considering legislation in support of smart grid technology to not only increase energy system resilience, but also improve reliability and efficiency. These policies can increase the reliability of the electrical grid by improving the management of electricity demand and by

allowing utilities to locate and address failing equipment or power outages more quickly. This technology comes with drawbacks, however, as it opens a door to cyberthreats.

As with many aspects of life, the electrical grid is increasingly interconnected. Millions of new intelligent components are operating in conjunction with legacy equipment that was not designed with modern cybersecurity in mind. These modernization efforts are changing the dynamics of the grid, connecting customer-based smart grid devices and utility control systems to the Internet. While this increased connectivity leads to improved efficiency and grid performance, it also increases the vulnerability to cyberattacks.

The scope of this threat has increased substantially in recent years—with persistent and documented cyber-intrusions into the power grid's critical infrastructure and control systems—leaving some experts to warn that the U.S. power sector is underprepared.[3]

Given that smart grid technologies are considered integral to establishing a 21st century grid, most of the cybersecurity legislation proposed in 2015 revolved around the creation of cybersecurity task forces or committees to study the issue and make recommendations on how to minimize these threats. All of this comes as concerns linger about the physical security of the nation's energy supply. At least 15 bills were introduced in 2015 that address the threat of electromagnetic pulse (EMP) attacks, and at least five bills exempt critical information about the grid and public utilities from disclosure under the Freedom of Information Act.

In all, more than 200 bills relating to energy security and resiliency were introduced in statehouses across the United States in 2015. These state policies play an important role in hardening infrastructure and preparing for disaster response in the event of disruptions and emergencies.

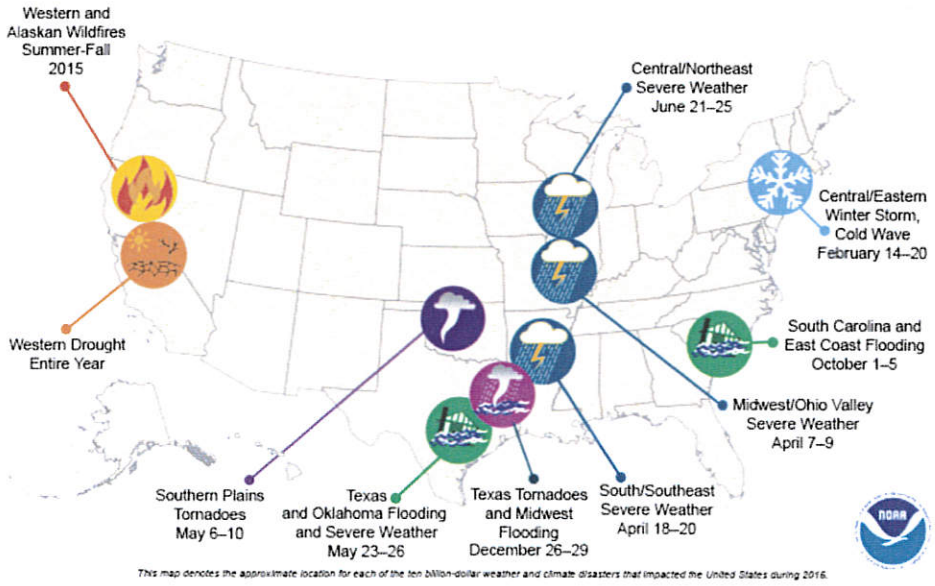
Disaster Preparedness

States have taken a number of steps to ensure that lights will stay on and water will continue to flow in the event of an emergency. These range from requiring standby generators at certain critical facilities to making it easier for out-of-state workers to help with disaster response.

Concerns are growing over the frequency and intensity of natural catastrophes. Data from the U.S. Department of Energy (DOE) shows that weather-related blackouts in the United States doubled between 2003 and 2012. In that same period, 679 widespread power outages occurred due to severe weather, at an annual cost of between $18 billion and $33 billion (Figure 1), according to a report issued by the Department of Energy.[4]

The Atlantic seaboard—where the U.S. Geological Survey says sea-level rise is occurring at rates three-times faster than the global average—is considered especially vulnerable. Two recent reports have compiled information on a number of coastal metropolitan regions, and assessed the vulnerabilities to energy infrastructure by combining factors of sea-level rise and storm surge. The report from the DOE Office of Electricity Delivery and Energy Reliability[5] found that infrastructure in certain regions—such as New York City, Houston and Miami—have a heightened level of risk. New York City alone has around 50 substations and 33 power plants that currently are located in areas that could be affected by rising seas and storms. A similar report by the Union of Concerned

Figure 1. U.S. 2015 Billion-Dollar Weather and Climate Disasters



Scientists[6] found that more than 400 major substations and nearly 70 power plants currently are exposed to flooding from hurricanes and storm surge in five metropolitan regions.

This trend is expected to continue and even increase in the coming decades. A flurry of recent studies have explored this issue and found that major storms are expected to occur more frequently,[7] and that the resultant flooding will be more severe by the close of the century.[8] A report commissioned by the Massachusetts Senate[9] warned that the state's infrastructure—including 12 power plants and LNG storage facilities located on land less than 10 feet below high tide—will face growing risks of flooding if steps are not taken quickly.

Nearly 40 percent of the U.S. population—over 123 million people—live in coastal shoreline counties, according to U.S. Census Bureau data.[10] Officials across the political spectrum in these communities are working to address the threat posed by rising seas and other concerns that could affect the electric grid. However, far from being a strictly coastal issue, nearly 20 cities across the United States—including Dallas, New Orleans, San Francisco, Norfolk and Pittsburgh—have hired a "chief resilience officer," whose role is to develop and lead a comprehensive resilience strategy.

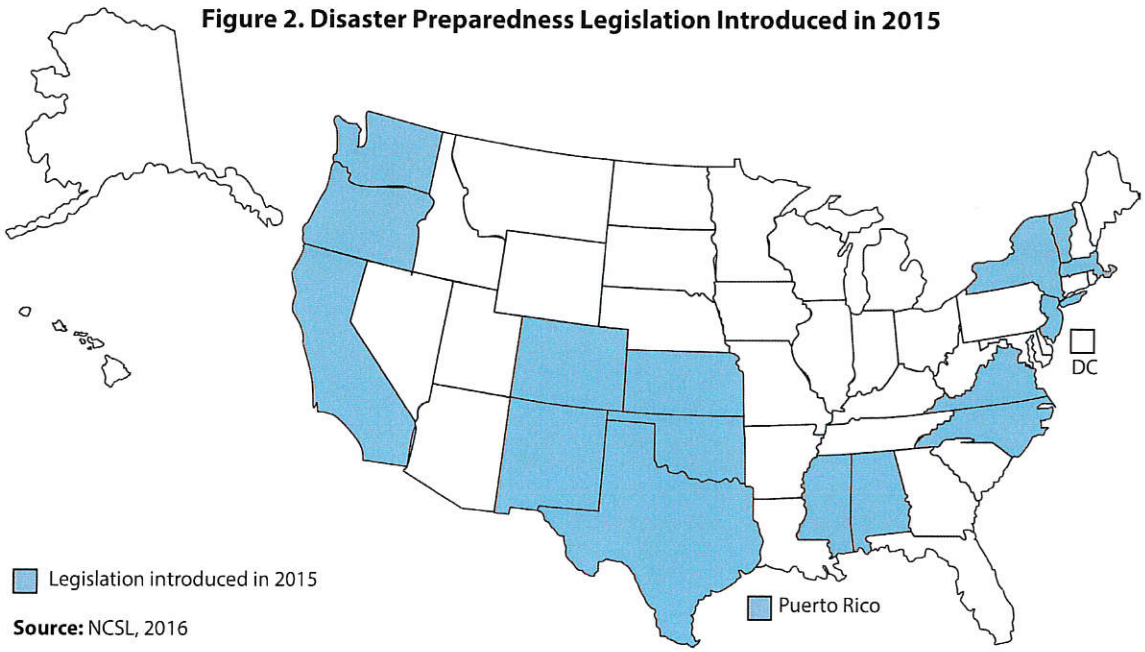
Lawmakers in 16 states and Puerto Rico introduced at least 29 bills to address disaster preparedness in 2015 (Figure 2), while 22 bills were introduced in 2014. Seven states—Alabama, Kansas, Mississippi, New Mexico, Oregon, Vermont and Virginia—introduced at least 12 bills that would exempt out-of-state workers and businesses from certain tax and registration requirements when they are responding to disasters.

At least 15 bills encouraged backup power generation, either by requiring that certain critical infrastructure or public shelters maintain backup generators or by offering incentives to residents who invest in energy-generating technologies. Two states—Oklahoma and Texas—proposed bills that would make it illegal for a homeowners' association to prohibit standby generators. At least four bills were intended to ensure access to motor and heating fuels in the event of an emergency. At least six bills relate to creating state response plans, and instruct state agencies to assess the grid's vulnerabilities and make recommendations.

Key bills from 2015

- **California** A.B. 184—(failed-adjourned) would provide energy efficiency and disaster preparedness guidance and assistance for small businesses.
- **Massachusetts**—Four bills (all pending) would establish a comprehensive adaptation management plan in response to climate change.

Figure 2. Disaster Preparedness Legislation Introduced in 2015



Source: NCSL, 2016

- **New Jersey**—A.B. 2579 (vetoed) would authorize municipalities to facilitate private financing of water conservation, energy improvements, storm shelter construction, and flood and hurricane resistance projects. Four bills (all pending) deal with backup generators and on-site generation for critical facilities. A.B. 2586 (vetoed) would establish a commission to study and make recommendations for improving the state's electric utility infrastructure.
- **New York**—A.B. 3007 (enacted) requires an energy audit and disaster preparedness review of residential health care facilities. A.B. 8390 and S.B. 5271 (both pending) would require the state, its political subdivisions, utilities and health care facilities improve preparedness and response and would require critical infrastructure to be protected.
- **North Carolina**—S.B. 436 (failed-adjourned) would direct the utilities commission to perform an assessment on the extent to which the state's electrical grid is prepared for an emergency.
- **Vermont**—H.B. 320 (enacted) establishes a petroleum set-aside system for liquid fossil fuels to be used in times of emergency or shortages.
- **Puerto Rico**—H.R. 108 (enacted) orders a comprehensive study of infrastructure, including systems for electricity, water and sewage, and other matters relating to security during a public disaster.

Key bills from 2014

- **New Jersey**—Five bills (all failed-adjourned) would require or offer incentives for installation of emergency generators at certain dwellings and facilities. Three bills (all failed-adjourned) would require public utilities to file emergency response and flood mitigation plans. Two bills (both failed-adjourned) would address the issue of motor fuel availability during emergencies. A.B. 1199 (failed-adjourned) would require electric distribution lines to be located underground in areas that are affected by severe weather or natural disasters.
- **New York**—A.B. 8387 (failed-adjourned) would direct several cities to conduct studies on the preparedness and readiness to respond to certain disasters.

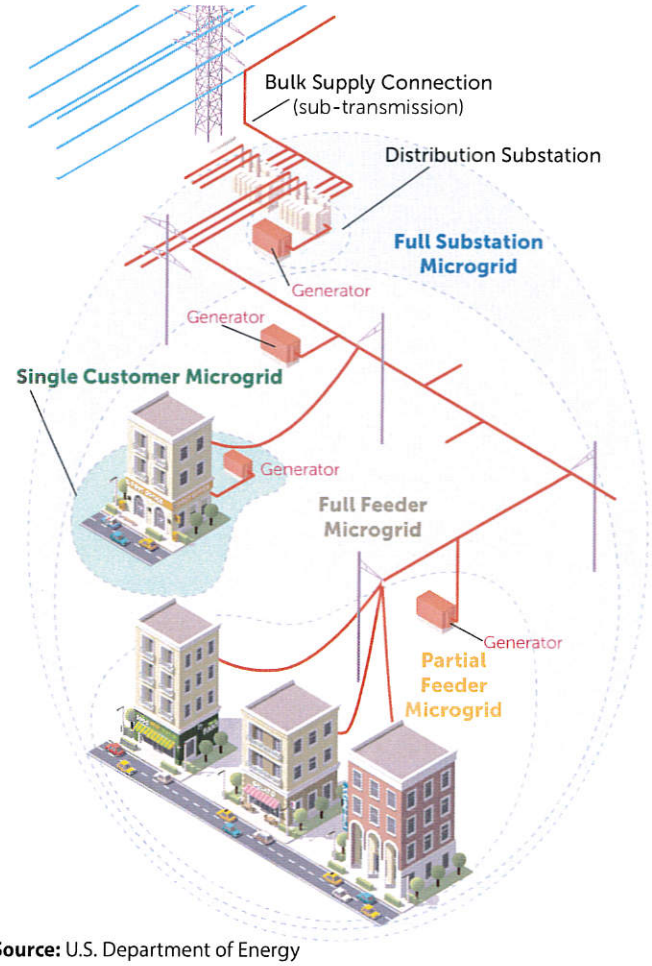
Microgrids

Legislators in at least 17 states introduced bills in 2015 that promote microgrids, often noting that these systems can serve an important role in an emergency. Microgrids can be designed in various ways and can include a variety of resources—utilizing everything from renewables to diesel generators—but they all provide independent power generation to a specific geographic area. The key resiliency component is the microgrid's ability to operate independently from the larger grid (Figure 3).

So, when a major power outage occurs, as happened in the aftermath of Superstorm Sandy, a microgrid can supply homes and businesses with electricity. In fact, while Superstorm Sandy knocked out power for 8.7 million customers across 24 states, a microgrid known as "Co-op City" in the Bronx was able to provide heat, electricity and hot water for 60,000 residents. Similarly, Princeton University and New York University were able to supply heat and power to parts of their campuses throughout the storm.

Figure 3. How a Microgrid Works

A system with its own power resources, loads and definable boundaries that can operate independently or in conjunction with the area's main electrical grid.



Source: U.S. Department of Energy

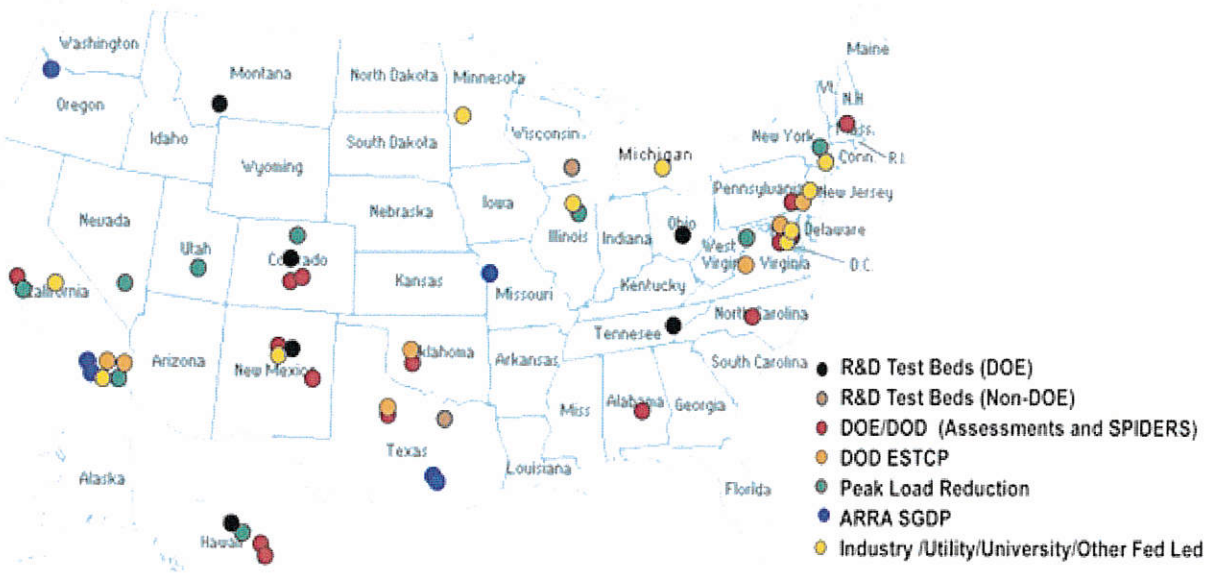
The East Coast is not the only area where microgrids are gaining ground. There are several federal initiatives through the DOE that support microgrid development across the United States (Figure 4). At the state level, bills emerged in a number of states that face hurricanes, earthquakes, tornados, winter storms and other threats. In the West, wildfires have been a regular cause of power outages in recent years, and some California tribes have developed microgrids that expand access to electricity in rural areas and help prepare for emergencies. On several occasions, a Miwuk Indian-owned microgrid has proven its ability to supply its own power for up to 10 days without grid access during wildfires.

While much of the discussion about microgrids has centered on their use in disaster scenarios, some lawmakers have also noted their ability to help diversify sources of energy generation. At least 28 bills were introduced in 2015. At least 11 bills in six states—Alaska, Connecticut, Colorado, Massachusetts, Maryland and New Jersey—offered grants, loans or other incentives to encourage the development of microgrids or similar structures.

Key bills from 2015

- **California**—A.B. 1530 (pending) would promote deployment of clean distributed energy and prioritizes deployment of smart grids and microgrids.
- **Connecticut**—H.B. 6991 (enacted) authorizes the Connecticut Green Bank to help finance energy improvements, including clean energy resources used in the creation of a microgrid, along with any related infrastructure.
- **Hawaii**—H.B. 264 (pending) would require the Public Utilities Commission to establish a process for electricity consumers to form microgrids to provide secure and reliable power when the central grid is down. Three resolutions urged utilities and the Public Utilities Commission to adopt policies that would support microgrids.
- **Illinois**—H.R. 3327 (pending) would require a report and workshops to illustrate how development of microgrids could strengthen the electric grid through reliance on the diverse supply options.

Figure 4. U.S. Department of Energy Microgrid Landscape



- **Maryland**—H.B. 1087 and S.B. 398 (both enacted) establish a pilot program for community solar.
- **Minnesota**—H.B. 3a (enacted) makes changes to energy provisions and requires that utilities issue reports that outline investments considered necessary to modernize and enhance the reliability of the grid, including energy storage and microgrids.
- **New Jersey**—At least eight bills have been introduced over the past two years that require or encourage backup generators. A.B. 4180 and S.B. 2691 (failed-adjourned) would establish microgrid pilot programs to equip critical public facilities with microgrids.
- **New York**—A.B. 6746 (pending) would require the Public Service Commission to develop recommendations for establishing microgrids, including critical buildings and the geographic areas where microgrids should be a priority.
- **Washington**—H.B. 1095 (enacted) requires a life-cycle cost analysis before construction or renovation of critical government facilities to determine the potential for combined heat and power systems that are able to serve public health and safety during a natural disaster or other emergency in which there may be a widespread power outage.

Distributed Generation and Diversification

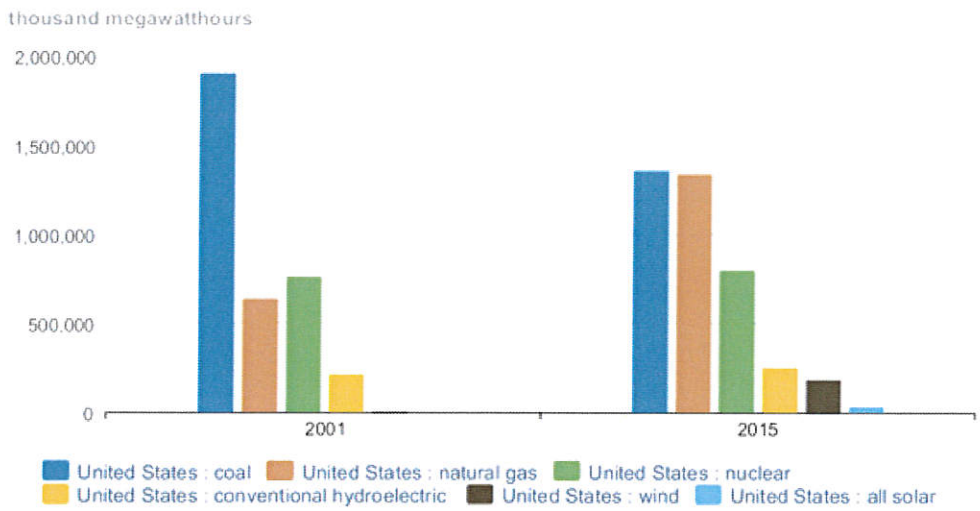
Distributed generation—power generation at the point of consumption—can help keep the lights on during a disaster. In addition, these resources have the potential to lower a utility's peak load, which can improve reliability.[11]

In crafting legislation, however, some lawmakers also used the concept of distributed generation to call for the continued diversification of state energy portfolios (Figure 5). The West Coast—and Hawaii, in particular, where electric rates are higher than in any other state due to dependence on imported fossil fuels for electricity generation—pushed this message by offering incentives to invest in renewables as a means of achieving energy independence. Other states encouraged diversification of the energy supply through coal, natural gas, biomass, offshore wind, nuclear and waste-to-energy.

Key bills from 2015

- **California**—S.B. 350 (enacted) requires an increase in the amount of electricity generated and sold from renewable energy resources in order to strengthen the diversity and resilience of the electrical system.
- **Hawaii**—H.B. 1273 (enacted) authorizes the construction of hydroelectric facilities of not more than

Figure 5. Net Generation for all Sectors, Annual



Data Source: U.S. Energy Information Administration

500 kilowatts on agricultural lands. H.B. 1286 (enacted) encourages energy efficiency, renewable energy and a reduction in state dependence on fossil fuels. S.B. 1050 (enacted) allows utility customers to elect to participate in renewable community energy projects. S.B. 1047 (pending) would authorize bonds to help develop a waste-to-energy plant.

- **New York**—A.B. 107 (pending) would require the development of a statewide shared renewable energy zone map and would provide for the interconnection of shared solar, farm waste, micro-combined heat and power, fuel cell, micro-hydroelectric and wind generation.
- **Ohio**—H.C.R. 9 (enacted) establishes a sustainable energy abundance plan to meet future energy needs, including new nuclear generation technology.
- **Utah**—S.B. 280 (enacted) promotes development of diverse energy resources, including nonrenewable and renewable resources, nuclear and alternative transportation fuels.
- **Vermont**—H.B. 40 (enacted) creates a program for electric utilities, sets certain requirements for renewable energy or renewable energy credits, and encourages distributed generation.
- **Virginia**—S.B. 1349 (enacted) requires that electric utilities file integrated resource plans in order to diversify their generation supply portfolio.
- **Washington**—Three bills—H.B. 1897 (enacted), S.B. 5024 (enacted), and H.B. 1912 (pending)—extend or would extend incentives for renewable energy and encourage or would encourage development of clean energy. S.B. 5113 (pending) would support small modular reactor siting and development.

In addition, at least nine bills sought to study or develop energy storage. Energy storage has been viewed as another form of redundancy in the grid, with the potential to provide backup power in the event of an outage by storing electricity in batteries. Several states also have sought to explore the possibility of vehicle-to-grid technologies, which would allow electric vehicles to supply backup power to the electric grid in the event of an energy shortfall or outage. Another seven bills addressed alternative fuels.

Key bills from 2015

- **California**—Three bills (all pending) would address energy storage and require the Public Utilities Commission to study energy storage and the role that electric vehicles could play. Three bills (all failed) would promote alternative fuels by adopting a renewable gas standard or providing support to in-state production of alternative fuels.
- **Connecticut**—S.B. 1078 (enacted) requires the state to seek proposals that provide for passive demand response, including energy storage solutions. Two other bills addressed energy storage and the role of electric vehicles.
- **Hawaii**—S.B. 349 (vetoed) would have established a renewable fuels production tax credit to encourage local production of renewable fuels.
- **Massachusetts**—H.B. 2852 and S.B. 1770 (both pending) would offer tax exemptions and other promotions to encourage community shared solar systems and energy storage programs.
- **Minnesota**—H.B. 1320 (pending) would establish a rebate plan to encourage purchase of energy storage

systems that can help with load management. H.B. 2081 and S.B. 1948 (both pending) would require public utilities to file plans that promote electric vehicles and would require a pilot program for vehicle-to-grid technology.

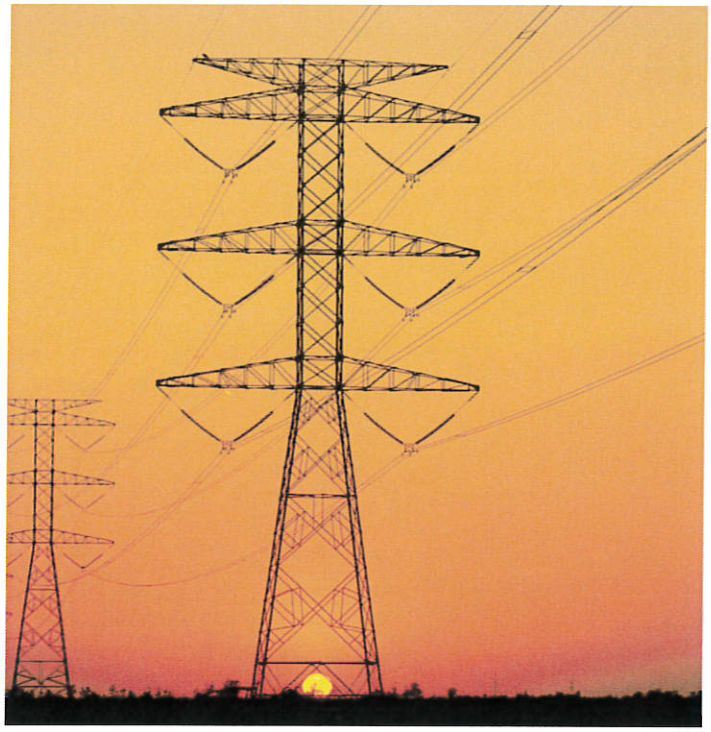
- **Oregon**—H.B. 2193 (enacted) directs electric companies to procure energy storage systems, allowing them to recover all costs through electrical rates.

Comprehensive Plans and Utilities

The electrical grid is undergoing rapid transformations, and states are playing a major role in that development. There is momentum across the country to modernize the grid. This often refers to the promotion of smart grid technologies, which allow customers and utilities to use energy more effectively and efficiently. In 2015, legislators in six states introduced at least 12 bills outlining comprehensive plans to modernize the electrical grid and make it more reliable through a combination of policies that promote energy efficiency, demand-response programs and on-site generation.

Key bills from 2015

- **California**—S.B. 83 (enacted) requires public utilities to enact net metering tariffs to enhance diversification and reliability of the state's energy resources and to encourage private investment in renewable energy and energy efficiency.
- **Illinois**—S.B. 1879 (pending) would establish a renewable energy fund, photovoltaic requirements, voltage optimization, demand-response, net metering, microgrids and low-income programs.
- **Minnesota**—H.B. 3a (enacted) requires that utilities issue reports every other year that describe transmission and distribution plans that outline investments considered necessary to modernize and enhance the reliability of the grid, including improvements to physical and cybersecurity, net metering, control technologies, energy storage, demand-response and microgrids.
- **New Hampshire**—H.B. 362 (enacted) requires each utility to file a resource plan in which it forecasts future demand; assesses energy management and supply options; and assesses distribution and transmission requirements, including benefits and costs of smart grid



technologies and other programs to ensure a more reliable and resilient grid. H.B. 614 (enacted) implements the goals of the 10-Year Energy Strategy, which include grid modernization.

- **New York**—A.B. 2371 (pending) would address aging infrastructure, establish a grid modernization program and create the Smart Grid Advisory Council.
- **Rhode Island**—S.B. 2439 and H.B. 7991 (both enacted) establish a framework for the state to coordinate with other New England states to make strategic investments in resources and infrastructure.

Another 21 bills introduced in 2015 required specific grid updates to improve system reliability. These actions include requiring utilities to file plans for the acquisition of smart grid technologies, requiring public utilities commissions to consider changes to the regulatory structure in light of distributed generation, and authorizing the development of regional organizations to improve reliability and efficiency.

Key bills from 2015

- **California**—A.B. 793 (enacted) requires weatherization and electrical and gas corporations to develop programs for acquisition of certain technology. S.B. 155 (pending) would authorize the independent system operator to enter into a multistate entity that would enhance the reliability and supply of the electrical grid.
- **Colorado**—S.B. 120 (pending) relates to a requirement that each provider of retail electric service in Colorado develop an electric grid modernization plan.
- **Illinois**—H.B. 3975 (enacted) provides for upgrades and modernizes the state's transmission and distribution infrastructure, including smart grid electric system upgrades.
- **Minnesota**—H.B. 2032 (pending) would require a study of the feasibility of creating a state public power authority with the power to construct and operate electric generation and transmission facilities.
- **Virginia**—H.B. 2237 and H.B. 1334 (both enacted) allow utilities to set rate increases to recover the costs of installing solar energy facilities and making improvements to the distribution system.
- **Washington**—H.B. 1895 (pending) would require electrical companies to file a smart grid technology report.

Cybersecurity

Since the U.S. Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT) began publishing reports in 2011, the energy sector has been the most targeted sub-sector of all U.S. critical infrastructure.[12] The energy sector has gone from being the target of nearly 60 percent of reported incidents in 2013 down to 16 percent in 2015,[13] when attackers turned their attention to industrial control system vendors.[14] A successful attack on a vendor could compromise vendor devices and provide access to power sector industrial control systems that regulate power management. This exemplifies how cyberthreats are evolving, requiring diligent surveillance and constant adaptation. More than half of all reported incidents were advanced persistent threats or sophisticated actors, according to ICS-CERT.

The nation's energy infrastructure faces a new range of threats as grid modernization efforts bridge the gap between two very different generations of technologies. "New components will operate in conjunction with legacy equipment that may be several decades old, and provide little to no cyber security controls," according to a report from the Electric Power Research Institute (EPRI).[15] In addition, information technology and operations technology have converged, linking computer systems with physical, equipment-oriented technology.

Concerns exist about what this means for the U.S. grid. Several high-profile incidents have proven that malware and other cyberthreats can result in physical damage to equipment and even service disruptions. However, most of these examples have occurred in areas of the world without the same level of cyberdefenses which have been deployed in the United States. In fact, an ICS-CERT 2015 report notes that, while there continue to be a number of incidents that result from "insufficiently architected networks," there have also been signs of significant improvement, given that nearly 70 percent of reported incidents had no evidence of successful intrusion by attackers. Attackers were almost 20 percent more successful at intruding networks in 2014.[16]

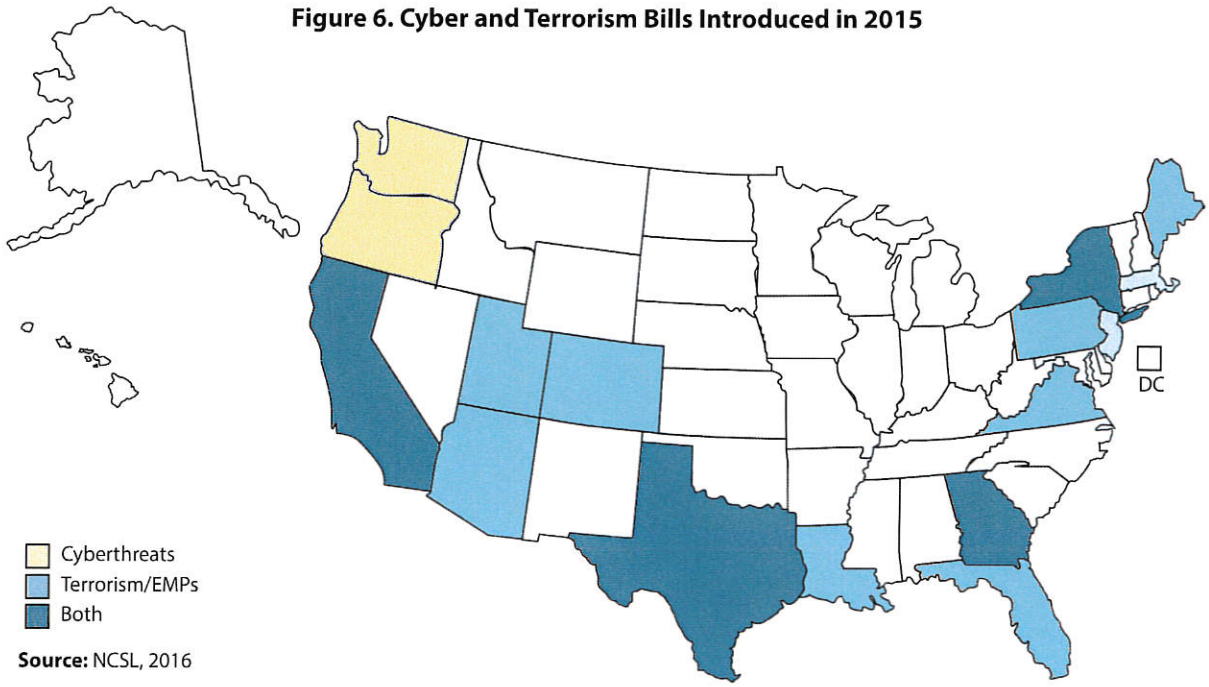
Supervisory control and data acquisition (SCADA) systems are one type of industrial control which are of particular concern. SCADA systems, in use since the 1970s, allow for the remote control of complex system operations over a wide territory. However, these systems were not designed with the Internet—let alone cybersecurity—in mind, and there have been documented incidents in which SCADA systems have been compromised through malware.

It will be decades before legacy equipment is phased out. In the meantime, EPRI suggests that systems be designed and implemented with cybersecurity as a primary concern.[17] "Cyber security must be included in all phases of the system development life cycle, from the design phase through implementation, operations and maintenance," according to another EPRI report.

To address these vulnerabilities, the electric power industry has been coordinating with the North American Electric Reliability Corporation (NERC) and federal agencies such as the National Security Agency (NSA), the Federal Energy Regulatory Commission (FERC), the U.S. Department of Homeland Security and the U.S. Department of Energy. FERC has approved new cybersecurity standards developed by NERC that aim to enhance the grid's protections. These updated standards—Critical Infrastructure Protection Version 5 (CIP V5)—are considered more robust and proactive. Previous versions applied only to utilities of a certain size, but CIP V5 affects the grid at all levels.

Although the federal government plays a significant role in countering these threats, utilities and states are also taking steps to strengthen cyberdefenses. Not only do states participate in NERC-sponsored grid security exercises like GridEx, but many also are exploring ways to address grid vulnerabilities and ensure that state response agencies are prepared. At least 16 bills or resolutions sought to address the issue at the state level in 2015 (Figure 6).

Figure 6. Cyber and Terrorism Bills Introduced in 2015



Source: NCSL, 2016

Key bills from 2015

- **California**—A.B. 853 (pending) would require that utilities use their own employees for work involving computer and other critical systems of nuclear, electrical and gas infrastructure in order to protect the integrity and security of the state's critical infrastructure. A.B. 1172 and A.B. 2200 (both pending) would require the state's Cyber Security Task Force to meet quarterly, and would create the Cyber Security Steering Committee within the governor's Office of Emergency Services.
- **Georgia**—Five bills (all pending) would create committees to address cybersecurity.
- **New York**—A.B. 6130 and S.B. 3407 (both pending) would require formation of a cybersecurity advisory board. A.B. 6133 and S.B. 3405 (both pending) would require a comprehensive review of all cybersecurity services to be performed every five years.
- **Oregon**—H.B. 3394 (pending) would establish a cybersecurity task force.
- **Washington**—H.B. 1468 (pending) would grant the governor authority to proclaim a state of emergency in the event of a cybersecurity incident. H.B. 1470 (pending) would establish a blue-ribbon panel on cybersecurity.

Terrorism

Physical threats to the power grid and other critical infrastructure also concern many lawmakers. At least 15 bills were introduced in 2015—and another four the previous year—aimed at protecting the electrical system against an electromagnetic pulse (EMP) attack. Of these, five states—Colorado, Georgia, New Jersey, New York and Texas—considered legislation that would have created committees to study the vulnerabilities and effects of an EMP attack and to evaluate technologies to address those issues. Meanwhile, three states—Florida, Pennsylvania and Texas—urged federal action to harden the grid against such attacks.

At the same time, at least five bills were introduced that exempted certain detailed information about the grid, utilities and state energy infrastructure from disclosure under the Freedom of Information Act. Four of these bills passed—in Arkansas, California, Kansas and Virginia.

Key bills from 2015

- **Massachusetts**—H.B. 3526 (pending) would require electric companies to develop and implement plans to address the vulnerabilities of the electrical grid to natural and EMPs and other manmade and natural occurrences.
- **New York**—A.B. 6657 and S.B. 2385 (both pending) would empower the state to decide if the sale, lease or operation of any critical infrastructure owned by the state would threaten public security, and creates the Critical Infrastructure Advisory Council.
- **Virginia**—S.B. 1238 (enacted) requires the state Department of Emergency Management to specifically plan for disasters caused by EMPs and geomagnetic disturbances.
- **Utah**—H.J.R. 26 (enacted) requires a study of the steps Utah has taken to protect its electrical grid and to examine work done in other states.

Key bills from 2014

- **Arizona**—S.B. 1476 (enacted) requires the state Department of Emergency and Military Affairs to develop preparedness recommendations in the event of an EMP.
- **Louisiana**—S.R. 169 (adopted) requests the governor's Office of Homeland Security and Emergency Preparedness to study the potential threats and consequences of an EMP.
- **Virginia**—S.J.R. 61 (enacted) directs the Joint Commission on Technology and Science to study the nature and magnitude of potential threats caused by geomagnetic disturbances and EMPs and to recommend strategies to protect infrastructure.

Funding

Lawmakers in five states introduced at least 10 bills to help fund improvements to the state electrical grid that would enhance energy security, reliability and resiliency. Hawaii introduced five of these bills, three of which have been enacted.

Key bills from 2015

- **Hawaii**—H.B. 1513 (enacted) establishes a two-year matching grant pilot program to strengthen local

companies that are conducting renewable energy research and development in order to reduce the state's dependence on fossil fuels. S.B. 359 (enacted) requires that 15 cents of the tax on each barrel of petroleum be deposited into the Energy Security Special Fund, and that 10 cents on every barrel be deposited into the Energy Systems Development Special Fund. S.B. 892 (enacted) appropriates money for resilience and sustainability strategy, including $25 million to improve efficiency, grid operations and resiliency.

- **New York**—A.B. 5883 (pending) would establish the New York State Infrastructure Development Bank, and would appropriate $250 million to support infrastructure improvement projects.
- **Washington**—H.B. 115 (enacted) allocates funds, including $28 million for grants to advance clean energy and enhanced transmission and distribution control systems, and for utility projects that demonstrate smart grid technologies.

Notes

1. American Society of Civil Engineers, *2013 Report Card for America's Infrastructure 2013* (Reston, Va.: ASCE, March 2013), http://www.infrastructurereportcard.org/energy.

2. Arup, Regional Plan Association (RPA) and Siemens, *Toolkit for Resilient Cities: Case Study: New York City Electrical Grid (n.p.: Siemens, 2013),* http://w3.siemens.com/topics/global/en/sustainable-cities/resilience/Documents/pdf/Toolkit_for_Resilient%20Cities_NY_Case_Study.pdf.

3. Richard J. Campbell, *Cybersecurity Issues for the Bulk Power System* (Washington, D.C.: Congressional Research Service, June 10, 2015), https://www.fas.org/sgp/crs/misc/R43989.pdf.

4. U.S. Department of Energy, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages* (Washington, D.C.: U.S. DOE, August 2013), http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

5. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, *Sea Level Rise and Storm Surge Effects on Energy Assets* (Washington, D.C.: U.S. DOE, n.d.), http://icfgeospatial.maps.arcgis.com/apps/MapSeries/index.html?appid=58f90c5a5b5f4f94aaff93211c45e4ec.

6. Union of Concerned Scientists, *Lights Out? Storm Surge, Blackouts, and How Clean Energy Can Help* (Cambridge, Mass.: Union of Concerned Scientists, 2015).

7. Anita J. Reed et al., "Increased threat of tropical cyclones and coastal flooding to New York City during the anthropogenic era," *Proceedings of the National Academy of Sciences* 112, no. 41 (Oct. 13, 2015).

8. Christopher M. Little et al., "Joint projections of US East Coast sea level and storm surge," *Nature Climate Change* 5 (Sept. 21, 2015): 1114-1120.

9. Commonwealth of Massachusetts, Report of the Senate Committee on Global Warming and Climate Change, *No Time to Waste* (Boston: Massachusetts General Court, Feb. 13, 2015), http://archives.lib.state.ma.us/handle/2452/264298.

10. National Oceanic and Atmospheric Administration, *NOAA's State of the Coast* (Washington, D.C.: NOAA, 2010), http://stateofthecoast.noaa.gov/.

11. U.S. Department of Energy, *The Potential Benefits of Distributed Generation and Rate-Related Issues That May Impede Their Expansion* (Washington, D.C.: U.S. DOE, February 2007), https://www.ferc.gov/legal/fed-sta/exp-study.pdf.

12. U.S. Department of Homeland Security, "Industrial Control System Cyber Emergency Response Team (ICS-CERT)," *ICS-CERT Monitor* (September 2014-February 2015), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

13. U.S. Department of Homeland Security, ICS-CERT, "Notable Incident," *ICS-CERT Monitor* (November-December 2015), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT%20Monitor_Nov-Dec2015_S508C.pdf.

14. U.S. Department of Homeland Security, ICS-CERT, "Trends in Incident Response in 2013, *ICS-CERT Monitor* (November-December 2013), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf.

15. Electric Power Research Institute (EPRI), *Risk Management in Practice: A Guide for the Electric Sector* (Palo Alto, Calif.: EPRI, Dec. 15, 2015), http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002003333.

16. U.S. Department of Homeland Security, ICS-CERT, "Notable Incident."

17. EPRI, *Cyber Security Strategy Guidance for the Electric Sector* (Palo Alto, Calif.: EPRI, May 30, 2012), http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001025672.

NATIONAL CONFERENCE *of* STATE LEGISLATURES

William T. Pound, Executive Director

7700 East First Place, Denver, Colorado 80230, 303-364-7700 | 444 North Capitol Street, N.W., Suite 515, Washington, D.C. 20001, 202-624-5400

www.ncsl.org

©2016 by the National Conference of State Legislatures. All rights reserved.

ISBN 978-1-58024-851-8

APPENDIX D.6
FINANCE COMMITTEE

FINANCE COMMITTEE STRATEGIC PLAN

Chair: Owen LaChat | Co-Chair: Tom Fite

September 2018
Indiana Executive Council on Cybersecurity

Finance Committee Plan

Contents

Committee Members **4**
Introduction **6**
Executive Summary **8**
Research **10**
Deliverable: Cyber Training (Ivy Tech) **14**
General Information 14
Implementation Plan 16
Evaluation Methodology 21
Deliverable: Top Security Tips Material **23**
General Information 23
Implementation Plan 24
Evaluation Methodology 27
Supporting Documentation **29**

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Owen LaChat	MutualBank	Technology Infrastructure & Security Manager	Chair	Voting
Tom Fite	Indiana Department of Financial Institutions	Director	Co-Chair	Advisory
William Tucek	Navient	Sr Mgr., Network Security	Full Time	Advisory
Brian Vitale	Notre Dame FCU	Chief Risk and Compliance Officer	Full Time	Advisory
Sharon Ferguson	MutualBank	Chief Risk Officer / ISO	Full Time	Advisory
Michael Servas	MutualBank	Sr. Information Security Analyst	Full Time	Advisory
Matthew Cloud	Ivy Tech	Project Director - TAACCCT Grant School of IT	Full Time	Advisory
Brad Stone	Indiana Department of Financial Institutions	Director of Information Technology	Full Time	Advisory
Kevin Stouder	Indiana Department of Financial Institutions	IT Program Lead/IT Examiner	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Determined the need for additional hands-on training and education of industry professionals on information security best practices and procedures. Spoke to industry professionals, vendors, and researched common training courses targeted to the financial industry.

- **Research Findings**
  - A need for increased and on-going training and education.

- **Committee Deliverables**
  - Cyber Training Program Pilot
  - Top Information Security Tips Material

- **Additional Notes**
  - A network penetration test of selected State systems conducted by members of the IECC and a state-run phishing portal for local and State government employees are being considered as potential deliverables in years two and three.

- **References**
  - Center for Internet Security – Controls
  - European Union – General Data Protection Regulation
  - Federal Deposit Insurance Corporation – Information Technology Risk Examination (InTREx)
  - Federal Deposit Insurance Corporation – Cybersecurity Assessment Tool (CAT)
  - Federal Deposit Insurance Corporation – Security Standards for Customer Information
  - Federal Trade Commission – Gramm-Leach-Bliley-Act
  - FFIEC – Information Technology Booklets
  - Financial Services – Information Sharing and Analysis Center
  - Ivy Tech – Cyber Security / Information Assurance Program
  - National Institute of Standards and Technology – Publications
  - Ponemon Institute – Cost of Data Breach Analysis
  - Ponemon Institute – Megatrends Study in Cybersecurity
  - SANS – CIS Critical Security Controls for Effective Cyber Defense
  - Verizon – Data Breach Investigations Report

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. The cybersecurity landscape has changed significantly over the past five years. As a result, members of the Finance Committee have taken a number of steps to focus on continually educating industry professionals on the basics of cybersecurity. We have been able to educate and train industry professionals through a number of professional organizations as well as through other informal discussions.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. There have been a number of significant cyber vulnerabilities that have affected financial institutions as well as other industries in the recent past. Among the most notable were the WannaCry ransomware attack, Meltdown/Spectre vulnerabilities, and the Heartbleed and Poodle attacks. It is hard to qualify or quantify the most significant cyber vulnerabilities until they have happened. Therefore, it is our responsibility to continually drive conversations within the financial industry around the risks of not following information security best practices.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. The greatest cybersecurity need and gap in the financial industry, as well as other industries, is to acknowledge and understand that cybersecurity risks are real, that they do occur, and they have real consequences. For example, we have witnessed and may have been impacted by the Equifax, Anthem, and Target breaches. Consequently, we need to remain diligent in the way that information is stored, processed, and transmitted and hold end-user employees and customers accountable for the confidentiality, integrity, and availability of information. Increased cybersecurity education is the greatest need, as it is through education that greater awareness can be achieved. This means educating the end-users, who are often the actual source of a breach. However, it also means more education for the technology specialists who will be continually challenged to identify and protect vulnerabilities as well as respond to and recover after an attack has occurred.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. There are a number of federal and state banking laws that the financial industry is beholden to including the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, and various Indiana Codes. Beyond domestic law, the European Union recently implemented the General Data Protection Regulation (GDPR). As a result of this new regulation, international corporations based here in America will have consequences for data protection issues that arise in Europe.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. There are a number of independent annual publications that report on the status of privacy, data protection, and information security policy. The Verizon Data Breach Investigations Report, Poneman's Cost of Data Breach Global Analysis, and Ponemon's Global Megatrends in Cybersecurity are three prominent examples. Each of these are linked above in the references section of the executive summary.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. There are a number of banking organizations that collect, document, and report on statistics and trends specifically for the financial industry. The American Bankers Associations (ABA), the Conference of State Bank Supervisors (CSBS), and the Independent Community Bankers Association (ICBA) are industry organizations who have accumulated data pertaining to cybersecurity risks in our area.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. The Cybersecurity Assessment Tool (CAT 1.0) was developed and released in recent years, and most recently updated in May 2017. CAT 1.0 was released jointly by state and federal regulatory parties as a tool that financial institutions could voluntarily use to identify risks and determine their cybersecurity maturity. Discussions are ongoing as to what the next version of this tool will look like. It is a challenge to develop such a tool that is sophisticated enough to be used by the larger community and smaller regional banks, yet also simple enough to be used by smaller banks with less complex systems and who also have less IT staff resources. The goal of CAT 1.0 was that the assessment could be completed internally by the institution's own IT staff, meaning it would not require third-party assistance. This philosophy was important, as the associated costs of using outside consultants would have greatly impacted the adoption rate of this assessment methodology.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Without a doubt, complete success in even as much as five years is unlikely. However, the trend of financial attacks, the severity of those attacks, and the loss of data from attacks should all be trending in a positive direction. Cybersecurity management tools will improve, reducing cyber exposure, and increased awareness will result in a greater end-user caution.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. Diligence and focused training are needed both in the corporate world and also with individual citizens. Access to training is key in a corporate world. Training is often targeted at IT specialists, and there is minimal training available for non-IT staff. Furthermore, access to what training is available can be expensive leaving corporations to decide between who gets access to training and to what extent. From a consumer standpoint, financial institutions recognize that a customer and a customer's access can be one of their greatest points of vulnerability. In response, institutions have started to educate their own customers to partner with their clients to reduce this exposure.
    b. A customized information security curriculum targeted towards financial sector professionals will increase cybersecurity.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. Access to cybersecurity specialists varies greatly across the country, as does the competition for and affordability of these resources. Larger metropolitan areas understandably have better access to a staff resource pool; however, demand for these resources is also greater in metropolitan areas. For example, access to and cost of staff would be greater in San Francisco than in Indianapolis, and likewise, access is greater in Indianapolis than it is in any small town in Indiana.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. The state of Indiana needs to continue its cybersecurity initiatives leveraging assets like its colleges and universities, research centers of excellence, and business communities. By leveraging these assets, the State can establish an environment that is conducive to attracting more cyber-based companies.

12. **What are your communication protocols in a cyber emergency?**
    a. The financial industry has a number of outlets with which to communicate cyber emergencies. One such outlet is the financial services – information sharing and analysis center (FS-ISAC). The FS-ISAC's mission is to protect the financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services. The FS-ISAC has protocols in place to manage rapid response communications during incidents.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. This is an expansive question, and probably should be a paper stand alone. Several different tools are available (National Institute of Standards and Technology (NIST) and CAT 1.0 for example); however, no platform serves a one size fits all solution. Given the wide range of complexity and risk variance across the industry, it would seem unlikely than any one set of best practices would fulfill the needs of all financial businesses.

Deliverable: Cyber Training (Ivy Tech)

Deliverable: Cyber Training (Ivy Tech)

General Information

1. **What is the deliverable?**
   a. Provide training on cybersecurity and prerequisite IT instruction for business executives to fully understand the risks and prevention of an active cyberattack.

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Giving industry professionals a solid, hands-on foundation in information security.

6. **What metric or measurement will be used to define success?**
   a. Certificate of completion of global IT and Cybersecurity Curriculum from CISCO on IT Essentials, Introduction to Networking, and CISCO Certified Networking Associate in CyberOps. Trainees will also be prepared for CompTIA A+, CompTIA Security+, and the CCNA CyberOps Certification. With one additional course they would be prepared for CompTIA Network+ and CISCO Certified Entry-level Network Technician.

7. **What year will the deliverable be completed?**
    a. 2019.

8. **Who or what entities will benefit from the deliverable?**
    a. Ivy Tech and various other public and private entities that attend the training courses.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Several other state colleges and universities have cybersecurity programs. Ivy Tech has 25 locations throughout the state to provide training. Ivy Tech courses could be taken by professionals for credit or taken in a fast track (one course per month) in a not-for-credit format. However, those who take it in a not-for-credit format obtain college credit by passing the industry certifications. All for-credit coursework or credit obtained by certification crosswalk taken during the cybersecurity program transfers to most Indiana four-year public universities. Additionally, this same coursework was approved by the Indiana Department of Education for students to take in the 9-12th grades in the new Computer Science and IT pathways and are dual credit eligible.
    b. Additional and higher-level cybersecurity training can be obtained through Ivy Tech towards an Associate of Science (AAS) degree in Cybersecurity which transfer as a 2+2 or 3+1 (3 years at Ivy Tech and 1 year at the four-year college) to four-year institutions for a Bachelor's degree focused on cybersecurity including Vincennes University, Purdue Northwest University, and WGU-Indiana.
    c. Through a National Security Agency (NSA)/National Science Foundation (NSF) grant, six students are chosen from the Ivy Tech CSIA program to receive free tuition and a $25,000/year stipend to complete their second year at Ivy Tech and last two years at Purdue Northwest. They are chosen after taken the mentioned three courses in this training program.
    d. Federal resources from the Department of Labor Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant established the initial data centers, IT specific classrooms, supplies and training needed to allow these programs to be available and increased the employment of over 20,000 IT students in three years in cybersecurity and other IT fields.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All other committees and working groups are encouraged to participate.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. The Ivy Tech program already exists and targeting it toward working professionals shouldn't need additional resources.
    b. However, targeting high school instructors so that the cybersecurity specific courses can be fully implemented within them will require $50K/year for two years to pay for trainers to train sufficient high school teachers across the State.

12. Who should be main lead of this deliverable?

a. Matthew Cloud

13. What are the expected challenges to completing this deliverable?

a. The cost of sending a business person (or teacher) through their respective training at Ivy Tech is $1,000 per person per course with a minimum of five people per course. There are several well-known private companies that offer cybersecurity training for industry professionals at a rate of $2,500-5,000 per person per course with a minimum of five to ten people. While Ivy Tech's cost is significantly less and achievable for larger businesses, the cost is too high for many high schools and smaller businesses including community credit unions.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Ivy Tech Curriculum & Scheduling	Matthew Cloud	100	July 2018	
Pilot courses & integrate other interested parties	Owen LaChat	30	February 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No.

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. The Ivy Tech program already exists and targeting it toward working professionals shouldn't need additional resources. However, targeting high school instructors for that the cybersecurity-specific courses can be fully implemented within the schools require $50K/year for two years. Funds will pay trainers to instruct a sufficient number of teachers across the state.

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes

17. What are the details of this deliverable?

a. The cost per person per course is $1,000. A minimum of five people per course is needed. MutualBank is funding at least five people for the pilot. Once the pilot is completed, it could be taught at any of the 25 campuses throughout the State in the faster format for business professionals, that is one class per month non-credit.

b. The fast track pilot for businesses began in July 2018 at the Ivy Tech Muncie campus, 345 S High Street Muncie, IN 47305, with one course per month.

c. Three courses are needed to complete the track:
   - Course 1 - IT Essentials.
   - Course 2 - Introduction to Networking.
   - Course 3 - CCNA CyberOps/Security+.

d. These courses have been taught for several years at Ivy Tech. The fastest these courses have been taught with typical college students is 8 weeks. They have been taught in four to six weeks for IT instructors for the past two years. As the pilot goes along, flexibility may be needed to extend the course length and will be given. The students in the pilot course, may talk with the instructor to change the start and end dates to work with any vacation. Classes will be recorded so that they can review later. Trainees will be expected to work online or at the campus 8-12 hours per week, in addition to the formal 4 hours of class time to successfully complete the work.

e. We have a primary instructor chosen who has taught two of the three classes for many years. We also have backup instructors for each of the courses and they have taught the courses for many years as well. Therefore, it will also help to see how well our current train-the-trainer model is working so that improvements can be made before adding high school instructors. Questionnaires will be sent to the trainees before and after on expectations and implementation so that future instruction will be improved.

f. Sustainability can be through grants such as Skill Up, NSF, or CISCO for high school instructors. Larger businesses should be able to afford the training. However, we should investigate a way to subsidize training for smaller businesses where most cybersecurity holes will occur. One possibility is a subsidy be generated by having enough people to be trained in a class through grants or otherwise. This would ensure the basic course costs are met. After that, a larger business could sponsor a "friend" business. As an example, when the minimum threshold for class cost coverage is reached, 10 trainees, then the number of trainees could be doubled at a minimal increased cost. As a maximum to ensure a quality experience, no more than 20 trainees in each class.
g. Additionally, Governor Holcomb recently signed a bill requiring high schools to include at least one Computer Science course for every high school student who starts by 2021.
h. Goal for 2021: Indiana to increase the number of instructors to at least one Computer Science (CS) teacher per Indiana high school. There are over 500, which include private. This would enable Indiana to educate these new CS instructors to teach cybersecurity at the end of a two-year process.
i. Goal for 2023: To have one cybersecurity trained instructor in each K12 school by 2023, so that between an integrated K14 system, Indiana will be reaching out to both K12 and businesses for supporting a statewide initiative. Then, we will have the most secure State in the US.

Benefits and Risks

---

18. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. See question #6.

19. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. With appropriate training and certifications, professionals working in critical infrastructure should be better prepared to recognize, assess, and respond to cybersecurity incidents within their organization. The average cost of a breached record is approximately $141. This does not include a company's reputational damage. The costs can become staggering for a company that houses personally identifiable information for thousands or millions of customers.

20. What is the risk or cost of not completing this deliverable?

a. Unknown. Educating the workforce of critical infrastructure is a necessity and should be considered a priority.

21. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Certificate of completion of global IT and cybersecurity Curriculum from CISCO on IT Essentials, Introduction to Networking, and CISCO Certified Networking Associate in CyberOps. Trainees will also be prepared for CompTIA A+, CompTIA Security+, and the CCNA CyberOps Certification. With one additional course they would be prepared for CompTIA Network+ and CISCO Certified Entry-level Network Technician.

22. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. **If Yes, please list states/jurisdictions**

i. Several other state colleges and universities have cybersecurity programs. Ivy Tech has 25 locations throughout the state to provide training. Ivy Tech courses could be taken by professionals for credit or taken in a fast track (one course per month) in a not for-credit format. However, those who take it in a not for credit format obtain college credit by passing the industry certifications. All for-credit coursework or credit obtained by certification crosswalk taken during the cybersecurity program transfers to most Indiana four-year public universities. Additionally, this same coursework was approved by the Indiana Department of Education for students to take in the 9-12th grades in the new Computer Science and IT pathways and are dual credit eligible.

ii. Additional and higher-level cybersecurity training can be obtained through Ivy Tech towards an AAS degree in cybersecurity which transfer as a 2+2 or 3+1 (3 years at Ivy Tech and 1 year at the four year college) to four-year institutions for a Bachelor's degree focused on cybersecurity including Vincennes University, Purdue Northwest University, and WGU-Indiana.

iii. Through an NSA/NSF grant, 6 students are chosen from the Ivy Tech CSIA program to receive free tuition and a $25,000/year stipend to complete their second year at Ivy Tech and last two years at Purdue NW. They are chosen after taken the mentioned three courses in this training program. Federal resources from the Department of Labor TAACCCT grant established the initial data centers, IT specific classrooms, supplies and training needed to allow these programs to be available and increased the employment of over 20,000 IT students in three years in cybersecurity and other IT fields.

23. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

b. **If Yes, please list states/jurisdictions**

i. That is a difficult question to answer accurately, as it is often not stated publicly exactly how a security breach occurred. I think it is safe to state that giving the professionals in the industry a solid technical foundation is extremely important.

Other Implementation Factors

24. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. See Question #4

25. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

26. What will it take to support this deliverable if it requires ongoing sustainability?

a. Ivy Tech or a similar state institution will need to continue offering their courses in a manner that is affordable and efficient for working professionals.

27. Who has the committee/working group contacted regarding implementing this deliverable?

a. Ivy Tech, Indiana Department of Financial Institutions, and Indiana Bankers Association.

28. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. Foundational knowledge of information security is not industry specific.

Communications

29. Once completed, which stakeholders need to be informed about the deliverable?

a. Whoever the IECC feels is appropriate.

30. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

31. What are other public relations and/or marketing considerations to be noted?

a. Planned marketing will occur via:
   i. https://www.ivytech.edu/it/
   ii. https://www.ivytech.edu/cyber-security/
   iii. https://www.ivytech.edu/itacademies/
   iv. Press releases regarding cybersecurity centers in Muscatatuck, Fishers, and Valparaiso.
   v. Directly to high schools and through statewide conferences for educators.
   vi. Campus-based advisory board meetings.

Evaluation Methodology

Objective 1: Ivy Tech will develop a cybersecurity curriculum for business executives by July 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Finance Committee and Ivy Tech will launch a pilot program with 7 participants by August 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☒ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Top Security Tips Material

Deliverable: Top Security Tips Material

General Information

1. **What is the deliverable?**
    a. Distribute training material relevant to explaining information security tips that could be implemented in a technology environment on an extremely limited budget that could help secure the environment's data from compromise.

2. **What is the status of this deliverable?**
    a. In-progress; 85% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Better end-user information security posture, education, awareness, reporting, and response.

6. **What metric or measurement will be used to define success?**
    a. A reduction of information security incidents overall.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Local and State governmental entities throughout Indiana.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. There are other information security resources available from various sources.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The material will be distributed to all working groups and committees, but their involvement won't be necessary.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. MutualBank, Inc.

12. **Who should be main lead of this deliverable?**
    a. Owen LaChat

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Revise & circulate "Top Information Security Tips" to IECC for mass distribution	Owen LaChat	85	December 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Better end-user information security posture, education, awareness, reporting, and response. A reduction of information security incidents overall.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. See question #5.

19. What is the risk or cost of not completing this deliverable?

a. Educating the workforce of critical infrastructure regarding information security best practices is a necessity and should be considered a priority.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Circulation of the material to a large audience. No baseline will be measured.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes.

b. **If Yes, please list states/jurisdictions**

i. Information security best practice documents are widely available. This document explains current attack techniques and potential mitigations. This document should be used in conjunction with other available resources.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes.
b. **If Yes, please list states/jurisdictions**
   i. See question #9

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. See question #4

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Nothing.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. The deliverable will be circulated internally to the committee to circulate as deemed necessary. This could include posting on a State website.

27. Can this deliverable be used by other sectors?

a. Yes,
b. **If Yes, please list sectors**
   i. Information security best practices are not industry specific.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Whoever the IECC feels is appropriate.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. Currently unknown.

Evaluation Methodology

Objective 1: IECC Finance Committee will develop the Top Information Security Tips training material for Indiana businesses by December 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

No Supporting Documentation Provided At This Time

APPENDIX D.7
GOVERNMENT SERVICES COMMITTEE

GOVERNMENT SERVICES COMMITTEE STRATEGIC PLAN

Chair: Superintendent Doug Carter | Co-Chair: John Davidson

September 2018
Indiana Executive Council on Cybersecurity

Government Services Committee Plan

Contents

Committee Members **4**
Introduction **6**
Executive Summary **8**
Research **11**
Deliverable: Indiana's Cybersecurity Hub Website **16**
General Information 16
Implementation Plan 17
Evaluation Methodology 21
Deliverable: Indiana Cyber Disruption / Emergency Plan **23**
General Information 23
Implementation Plan 24
Evaluation Methodology 28
Supporting Documentation **30**
Department of Revenue 31

Committee Members

Committee Members

Name	Title	Organization	Position	IECC Membership Type
Doug Carter	Superintendent	Indiana State Police	CHAIR	Voting
Chuck Cohen	Captain	Indiana State Police	CHAIR – PROXY	Voting Proxy
John Davidson	Supervisory Special Agent	FBI - Indianapolis Field Office	CO-CHAIR	Non-Voting
Tad Stahl	Director / Deputy Director for Cyber Intelligence	IN-ISAC / Indiana Intelligence Fusion Center	Full Time	Advisory
Kathy Dayhoff-Dwyer	District Coordinator Liaison	Indiana Department of Homeland Security	Full Time	Advisory
Paul Dvorak	Special Agent in Charge	United States Secret Service	Full Time	Non-Voting
Doug Swetnam	Section Chief	Indiana Attorney General	Full Time	Voting Proxy
Bryan Sacks	State Chief Information Security Officer	Indiana Office of Technology	Full Time	Advisory
David Murtaugh	Executive Director	Indiana Criminal Justice Institute	Full Time	Advisory
David Tygart	J36, INNG	Indiana National Guard	Full Time	Advisory
Ted Cotterill	Chief Privacy Officer and General Counsel	Management Performance Hub	Full Time	Advisory
Ryan Myers	Sergeant	Indiana State Police	As needed	Advisory
Chris Carter	Sergeant	Indiana State Police	As needed	Advisory
Adam Krupp	Commissioner	Indiana Department of Revenue	As needed	Voting
Connie Lawson	Secretary of State	Indiana Secretary of State	As needed	Voting
Tony Enriquez	Cyber Security Advisor	USDHS	As needed	Non-Voting
Patrick McCann	Special Agent	United States Secret Service	As needed	Non-Voting

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - National Institute of Standards and Technology (NIST) Standards and Roadmap
    - https://www.nist.gov/cybersecurity-framework
  - Indiana Department of Homeland Security (IDHS) Cyber Annex
  - Indiana State Police – Indiana Intelligence Fusion Center whitepaper
  - International Association of Chiefs of Police (IACP) Cybercrime and Digital Evidence Committee
  - Association of State Criminal Investigative Agencies (ASCIA) Cybercrime Committee
  - Federal Bureau of Investigation (FBI) Cyber Division documents and resources
  - Internet Crime Complaint Center (IC3) statistical information
  - National Domestic Communications Assistance Center documents and resources
  - National White Collar Crime Center documents and resources
  - U.S. Department of Homeland Security (USDHS) Cybersecurity Guidelines and Resources
  - Presidential Executive Order on Cybersecurity
    - https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
    - https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity
  - Information Sharing and Analysis Center (ISAC) – State Comparison Research
  - Multi-State Information Sharing and Analysis Center (MS-ISAC) documents and resources
    - https://www.cisecurity.org/ms-isac/
  - U.S. Computer Emergency Readiness Team (US-CERT) documents and resources
    - https://www.us-cert.gov/
  - Collection of Indiana State Agency Cybersecurity and Identity Protection Resources (In Process)

- **Key Research Findings**
  - There is a long-standing, effective, and robust existing partnership among federal, state, and local government services in the areas of investigating and providing first response to cyber incidents and cyber emergencies in Indiana. Additionally, a plethora of established and mature government services already exist at the federal and state levels for cybersecurity. Those services are well-known among those responsible for cybersecurity both in the private and public sectors.
  - The NIST Framework for Improving Critical Infrastructure Cybersecurity ("The Framework") provides a common language for understanding, managing, and expressing cybersecurity risk, both internally and externally.
  - It is likely that state/local governmental adoption of the Framework and Roadmap will be used as a metric for determination of the availability of federal grant

funding in several areas. This will ensure consistency in cybersecurity among states, and between state and the federal governments.
    - The NIST Framework can be used to benchmark where a component of state/local government is at on the NIST Roadmap, both in terms of its own cybersecurity and in terms of incentivizing private business cybersecurity efforts in the state, to federal funding.

- **Committee Deliverables**
    - Indiana's Cybersecurity Website Hub
    - Indiana Cyber Distribution/Emergency Plan

- **Additional Notes**
    - See linked sites (all retrieved on 01/02/2018)
    - The Government Services Committee members also may provide input on the Indiana Department of Homeland Security's Cyber Annex and Indiana Office of Technology Communications Breach Protocol.

- **References**
    - See linked sites (all retrieved on 01/02/2018)

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. ISP –
        i. National leadership on cybercrime forensics
        ii. Full-time cybercrime investigators who are network intrusion and cybercrime specialists
        iii. Robust and long-standing interaction with federal law enforcement agencies in the areas of cybercrime and cybercrime forensics
        iv. National and international leadership on policy, with personnel sitting on several national and international cybercrime and digital evidence groups.
        v. Indiana Intelligence Fusion Center (IIFC) development of cybercrime intelligence component under supervision of deputy director for cyber intelligence.
    b. IDHS – Drafted cyber annex and Crit-Ex
    c. U.S. Secret Service (USSS) – Provided and continues to provide nationwide cybercrime training to law enforcement, prosecutors and judges through training and education at the National Computer Forensics Institute at Hoover, Alabama.
    d. IOT –
        i. Working to bring the State in compliance with appropriate NIST framework
        ii. Launch of Security Operations Center (SOC) and IN-ISAC
        iii. Partnership with Indiana Intelligence Fusion Center in coordination of cybercrime intelligence and IN-ISAC/SOC
        iv. Established a State-Wide Training and Awareness Program
        v. Developed and communicated an effective body of Policy and Standards based off of NIST
        vi. Established strong governance through use of processes and development of committees (Policy Management Committee; Exception Management)
        vii. Significantly expanded resource and tooling for the teams to address gaps and new threats
    e. Attorney General (AG) – Consumer protection program and Identity Theft Credit Kit
    f. Indiana Department of Revenue (IDOR): Provided annual awareness training to all employees, contractors, temps, vendors; facilitated business continuity and incident response exercises; and disseminated notifications about real-world security events, issues and best practices to the entire agency.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Year-over-year, sophistication increases in phishing attacks. There is always an opportunity to refresh training and reinforce strong security awareness.
    b. IDOR: External threats, malicious insiders, employees who fall for social engineering schemes, and sensitive data outside of the State's protected zone.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Continued partnership among public and private sector actors responsible for cybersecurity and cyber emergency response.
    b. Coordination of messaging to private sector and local government related to available government services at the federal and state levels.
    c. Public being clearly aware of who to contact in case of a cyber emergency or incident, with the message that crime victims and those who experience potential network breaches should always contact law enforcement.
    IDOR: Funding and manpower to support security assessments and implementation of security enhancements.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Numerous federal and state laws related to responsibilities to safeguard Personal Identifying Information (PII) of third parties on networks and responsibilities to report certain crimes and events in an appropriate and timely manner.
    b. IDOR: Internal Revenue Service (IRS) publication 1075, National Institute of Standards and Technology (NIST) special publication 800-53 and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), State code, and state agency policy and standards.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Case studies include learning from other state's successes and failures in their cybersecurity efforts, including Michigan, Virginia, Maryland, and Massachusetts.
    b. Publicly available information on Madison County, Indiana malware attack.
    c. IDOR: The Information Security Research and Education (INSuRE) program researches and seeks solutions to hard security problems. INSuRE members are the US Intelligence Community, US National Laboratories, US universities and colleges such as Purdue, and State government organizations that include IOT.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. NIST Standards and Roadmap
        i. https://www.nist.gov/cybersecurity-framework
    b. IDHS Cyber Annex
    c. Indiana State Police – Indiana Intelligence Fusion Center whitepaper
    d. IACP Cybercrime and Digital Evidence Committee
    e. ASCIA Cybercrime Committee
    f. FBI Cyber Division documents and resources
    g. Internet Crime Complaint Center (IC3) statistical information
    h. National Domestic Communications Assistance Center documents and resources
    i. National White Collar Crime Center documents and resources
    j. USDHS Cybersecurity Guidelines and Resources

k. Presidential Executive Order on Cybersecurity
   i. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
   ii. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity
l. ISAC – State Comparison Research
m. MS-ISAC documents and resources
   i. https://www.cisecurity.org/ms-isac/
n. US CERT documents and resources
   i. https://www.us-cert.gov/
o. Collection of Indiana State Agency Cybersecurity and Identity Protection Resources (In Process)

7. What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?

a. See previous question.
b. IDOR: The IRS requires anyone receiving Federal Tax Information (FTI) to receive security awareness training, additional security training for specific roles, and contingency and incident response training for pertinent personnel.

8. What does success look like for your area in one year, three years, and five years?

a. Develop the Indiana Cyber Emergency Plan
b. Create a collaborative communications plan for the general public (individuals, local government, and businesses) about state and federal cybersecurity government services and resources, including centralizing information on www.in.gov/cybersecurity.
c. Provide input to Indiana Department of Homeland Security Cyber Response Annex to the Comprehensive Emergency Management Plan.
d. Provide input to Indiana Office of Technology Communications Breach Protocol for state agencies and recommended protocol for local government.
e. IDOR: Year 1: Implement performance of annual security assessments and security controls for severe and significant findings. Years 3 & 5: Help vendors, partners, and tax e-filing community become compliant with DOR security; improve agency access controls, data security, and vulnerability management; and normalize annual business continuity/disaster recovery planning and testing.

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

a. Create a collaborative communications plan for the general public (individuals, local government, and businesses) about state and federal cybersecurity government services and resources, including centralizing information on www.in.gov/cybersecurity.
b. IDOR: The public should be apprised that DOR continuously implements tools and processes to bolster cybersecurity to protect their information, which may appear inconvenient to them. For example, we may require taxpayers logging into our applications to increase the length and complexity of their passwords.

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. Many state agencies have cybersecurity-related workforce. For example, IDOR has:
   i. Total DOR Workforce as of December 2017: 751. We have 659 FTEs and 92 contractors.
   ii. Total DOR Cybersecurity Staff: 6
   iii. Total DOR Cybersecurity Staff shortfall: 0

11. What do we need to do to attract cyber companies to Indiana?

a. N/A

12. What are your communication protocols in a cyber emergency?

a. First call from victim or entity experiencing an emergency should be to enforcement. Enforcement will coordinate between State and federal enforcement resources. Other government services will be notified and activated ad hoc, i.e as necessary.
b. IDOR: We communicate based on our formalized process of identifying, analyzing, responding to, and recovering from incidents to include cyber emergencies

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. NIST Framework and Roadmap
b. IDOR: Defense in-depth: an information assurance concept in which multiple layers of security controls are placed throughout an information technology system; Initial and annual security awareness training; Phishing testing.

Deliverable: Indiana's Cybersecurity Hub Website

Deliverable: Indiana's Cybersecurity Hub Website

General Information

1. **What is the deliverable?**
   a. Improve the Cybersecurity website (www.in.gov/cybersecurity) and make it the central hub for cybersecurity information in Indiana

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Revamp the Cybersecurity website for the state and incorporate the marketing of the site in the public awareness working group communications plan

6. **What metric or measurement will be used to define success?**
   a. Completion of the cybersecurity website and monitoring website traffic

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. General public

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Public awareness and training working group

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IOT will host the cybersecurity hub website and assist in revamping it. Other state agencies and federal agencies link to cybersecurity information.

12. **Who should be main lead of this deliverable?**
    a. IECC Director

13. **What are the expected challenges to completing this deliverable?**
    a. Incorporating all the resources from state and federal agencies appropriately.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Create a Project Plan with IN.Gov, IOT, and IN-ISAC to create a new website	Cybersecurity Program Director	100%	May 2018	
Develop website content	Cybersecurity Program Director and content team	100%	August 2018	
Develop website framework	IN.gov	100%	August 2018	
Test website and make edits	Cybersecurity Program Director and content team	100%	August 2018	
Develop Communications Plan	Cybersecurity Program Director	100%	September 2018	
Website launches	IN.gov	100%	September 2018	
IECC members make edits and update website	IECC	0%	January 2019 – change package #1 March 2019 and on – scheduled change packets	Ongoing effort
Implement Communications Plan	Cybersecurity Program Director	25%	September 2018 – September 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1 FTE	1 FTE	Communications /Web master	State of Indiana	N/A	
1 FTE	0	Communications and/or cybersecurity	State of Indiana	N/A	Intern to assist IOT and Cybersecurity Program Director with website development and content

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
IN.Gov	Services will be required to create the website in the timeframe needed	N/A	N/A	State of Indiana – Indiana Office of Technology	N/A	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. This will provide a central location for the public and a variety of stakeholders to get and receive key information surrounding cybersecurity in Indiana, including but not limited to Indiana Emergency Disruption Plan, training, toolkits, cyber events, cyber tips, self-assessments, maturity models, and federal and state resources.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will provide the public and stakeholders a central hub for many resources that the IECC is developing that will decrease their cybersecurity risk through education, awareness, and training.

19. What is the risk or cost of not completing this deliverable?

a. The risk of not completing this deliverable is that the many resources that the IECC is developing for the public will not be easily found. If they are not found, then stakeholders may find it more difficult to raise their cybersecurity level.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. A completion of the website and meeting the milestones will be a measure of success. In addition, an increase of traffic to the website compared to the baseline of traffic to the current website will also be a measure of success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. Many states do have a central hub for its cybersecurity efforts. An example is Virginia at http://cyberva.virginia.gov/ or dedicated sections of websites such as Maryland at http://doit.maryland.gov/cybersecurity/Pages/default.aspx

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. Many other states do not have a central hub for cybersecurity efforts in the state

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Scope of project to be done by the deadline may negatively impact the deliverable.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. A state employee will need to serve as point person for all updates that will need to occur on the website.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Indiana Office of Technology, IN.Gov web services, IN-ISAC

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All sectors

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. General public, IECC members, state, federal, and local government, partners, legislative branch, executive branch, businesses, sectors

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. This will serve as the Central Hub for all other relative public relations and marketing on behalf of the IECC.

Evaluation Methodology

Objective 1: IECC will develop and launch a statewide cyber hub website by September 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Increase website traffic to www.in.gov/cyber by two-hundred percent by September 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Indiana Cyber Disruption / Emergency Plan

Deliverable: Indiana Cyber Disruption / Emergency Plan

General Information

1. **What is the deliverable?**
   a. Indiana Cyber Disruption/Emergency Plan

2. **What is the status of this deliverable?**
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☒ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Indiana Cyber Disruption/Emergency Plan created to formalize partnerships and processes to be used to communicate to stakeholders.

6. **What metric or measurement will be used to define success?**
   a. Completion of plan and communication of plan.

7. **What year will the deliverable be completed?**
   a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Government agencies and business stakeholders.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Emergency Services and Exercise working group, public awareness and training working group, cyber sharing working group, pre to post incident working group, and local government working group.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Law enforcement agencies (federal and state) and state agencies

12. **Who should be main lead of this deliverable?**
    a. Government Services Committee

13. **What are the expected challenges to completing this deliverable?**
    a. Getting consensus from all involved in proper notification and mass communicating it to stakeholders who would benefit from it.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Draft Plan	Tad Stahl	100%	November 2017	
Provide to Committee for review	Chuck Cohen	100%	November 2017	
Edit Plan	Cybersecurity Program Director	100%	August 2018	
Review and provide feedback on plan	Government Services Committee	75%	January 2019	
Finalize Plan	Cybersecurity Program Director	0	March 2019	
Distribute Plan	Cybersecurity Program Director	0	May 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A	N/A	State and federal agency leads	Government	N/A	Government leads will provide feedback on plan

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. This plan is the external communication piece to government partners, emergency service manager, business and the general public as to who to contact during a cyber emergency and what the roles of the various stakeholders involved will be.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will reduce the potential confusion during a cyber emergency with certain key stakeholders and the general public.

19. What is the risk or cost of not completing this deliverable?

a. The risk of not completing this deliverable is adding to the already confused stakeholders of who to contact and when. This is especially important when there is misinformation about who to contact, when in fact law enforcement should always be the first contact made during a cyber emergency.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion of all milestones and a comprehensive review from key state and federal agencies is considered a success for this plan.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. Michigan has a Cyber Disruption Plan that Indiana used as a reference point in creating this plan.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. There are other states that do not have a disruption plan. The National Governor's Association has a list.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Appropriate review of key state agencies in a timely manner may affect this deliverable.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. N/A

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All sectors can use this plan as a reference point in a cyber emergency.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. State and federal partners, local government, sector partners, associations, IECC members, emergency services partners, general public and businesses

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC Government Services Committee will develop the Indiana Cyber Disruption/Emergency Plan for the public by May 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Department of Revenue Government Services Research Responses

Department of Revenue
Government Services Research Responses

December 2017

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

COMMITTEE AND WORKING GROUP QUESTIONNAIRE – RESEARCH PHASE

Instructions: As your committee or working group is in the Research Phase, it is important we work with other committees and working groups to get the information your team will need to be successful. Please answer the questions the best you can.

Provide your questions and answers to MosleyCLM@iot.in.gov no later than ***January 2018.***

Committee/Working Group Completing Questions: Government Services Committee and Personally Identifiable Information (PII) Working Group

Person Submitting Answers: Adam Krupp, Commissioner, Indiana Department of Revenue

Email of Person Submitting: AKrupp1@dor.IN.gov

Date Submitted: December 2017

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Provided security awareness training to all FTEs, contractors, temps, and vendors at on-boarding and annually thereafter. This training apprises employees of the data they must protect, and the methods by which they must be protected.
    b. Led a Continuity of Operations plan exercise in 2014—next one projected for 2018
    c. Trained and exercised the Department of Revenue (DOR) Incident Response team and plan annually
    d. Sent periodic e-mails and published articles in agency publications apprising all DOR staff of security issues and best security practices
    e. Sent e-mails to all DOR staff apprising them of urgent real-world security issues, and how to address them (e.g., phishing messages and phone-based social engineering attacks)

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. External threats (State and non-state cyber actors, cybercriminals, cyberterrorists, etc.)
    b. Malicious insiders
    c. Employees who fall for social engineering schemes
    d. Servers containing sensitive data that reside outside of the state's protected zone (PZ)

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Funding and manpower to support security assessments and implementation of security enhancements

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Internal Revenue Service (IRS) Publication 1075
    b. National Institute of Standards and Technology (NIST) Special Publication 800-53: Using Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) for detailed security assessments
    c. Indiana Code and policies
    d. Indiana Office of Technology (IOT) policies and standards
    e. DOR policies and procedures

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. The Information Security Research and Education (INSuRE) program researches and seeks solutions to hard security problems. INSuRE members are the US Intelligence Community, US National Laboratories, US universities and colleges which include Purdue, and State government organizations including IOT.

6. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. All other state departments of revenue/taxation that receive Federal Tax Information (FTI) are required by IRS to provide:
        i. Security awareness training to all employees
        ii. Role-based training to personnel based on assigned security roles and responsibilities
        iii. Contingency training to personnel responsible for recovering backup copies of FTI
        iv. Incident response training to personnel responsible for handling and reporting security events

7. **What does success look like for your area in one year, three years, and five years?**
    a. **Year 1**
        i. Conduct security assessments
        ii. Implement security controls address severe and significant vulnerabilities and threats
    b. **Year 3**
        i. DOR, its vendors, partners, and e-filing tax community comply with DOR security requirements
        ii. Work towards the following goals
            1. All sensitive DOR servers reside in the state's PZ
            2. DOR servers reside in appropriate network segments
            3. All sensitive DOR data within the state network is encrypted at rest and in motion
            4. DOR users have least privileged access
            5. Security patching is done immediately
            6. Continuity of Operations (COOP) and Disaster Recovery (DR) plans are developed, appropriately resourced, and successfully tested
    c. **Year 5:** Achieve the following goals
        i. All sensitive DOR servers reside in the state's PZ
        ii. DOR servers reside in appropriate network segments
        iii. All sensitive DOR data within the state network is encrypted at rest and in motion
        iv. DOR users have least privileged access
        v. Security patching is done immediately
        vi. COOP and DR plans are developed, appropriately resourced, and successfully tested

8. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. The public should be apprised that DOR continuously implements tools and processes to bolster cybersecurity to protect their information, which may appear inconvenient to them. For example, we may require taxpayers logging into our applications to increase the length and complexity of their passwords.

9. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. Total DOR Workforce as of 17 Dec 2017: 751. 659 full-time employees (FTEs) and 92 contractors.
    b. Total DOR Cybersecurity Staff: 6
    c. Total DOR Cybersecurity Staff shortfall: 0

10. **What do we need to do to attract cyber companies to Indiana?**
    a. Unknown

11. What are your communication protocols in a cyber emergency?

a. DOR Employee, IOT, or anyone else identifies and reports suspicious activities to DOR Security Team
b. DOR Security Team assesses and analyzes the situation, and determines if there is an emergency
c. DOR Security Team, upon DOR Chief Information Officer (CIO) approval, takes immediate action as necessary to stop the perpetuation of damage
d. DOR Security Team develops multiple courses of action (COA) to address remaining security concerns and to recover from the event, then presents them to other members of the DOR Incident Response Team comprising DOR Chief Operating Officer, DOR Chief Information Officer, DOR Inspector General, DOR Legal Team, DOR Communications Team, and IOT Chief Information Security Officer
e. DOR Incident Response Team decides on a single course of action
f. DOR Incident Response Team briefs DOR Commissioner on the situation, actions taken, and proposed COA
g. DOR Commissioner approves COA
h. DOR Incident Response Team works with IOT to execute the approved COA

12. What best practices should be used across the sectors in Indiana? Please collect and document.

a. Defense in-depth: an information assurance concept in which multiple layers of security controls are placed throughout an information technology system
b. Initial and annual security awareness training
c. Phishing testing

APPENDIX D.8
HEALTHCARE COMMITTEE

HEALTHCARE COMMITTEE STRATEGIC PLAN

Co-Chair: Mark Lantzy | Co-Chair: Jacob Butler

September 2018
Indiana Executive Council on Cybersecurity

Healthcare Committee Plan

Contents

Committee Members **4**

Introduction **6**

Executive Summary **8**

Research **13**

Deliverable: Vendor Management **17**

General Information 17

Implementation Plan 18

Evaluation Methodology 23

Deliverable: Long-Term Education **25**

General Information 25

Implementation Plan 27

Evaluation Methodology 31

Deliverable: Indiana Threat Intelligence Distribution System **33**

General Information 33

Implementation Plan 35

Evaluation Methodology 39

Supporting Documentation **41**

IECC Healthcare Committee Jim Routh Meeting Notes 42

IECC Healthcare Committee Indiana Medical Device Manufacturers Council (IMDMC) Meeting Notes 46

IU Health Business Associate Agreement and Security Exhibit 48

Lasalle University Implementing Secure Cloud Computing in the Small to Medium-Sized Healthcare Environment 65

Temple University Improving Healthcare Provider Information Security Through the Implementation of Financial Systems Structures and Controls 141

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Mark Lantzy	Indiana University Health	SVP/Chief Information Officer	Chair	Voting
Jacob Butler	Parkview Health	Information Security and Compliance Specialist	Co-Chair	Advisory
Mitchell Parker	Indiana University Health	Executive Director, Information Systems	Chair Proxy	Advisory
David Day	Sallie Mae	IDM Manager	Contributing	Advisory
Paul McAninch	Indiana University Health	Director, Information Security and Compliance	Contributing	Advisory
Cliff Campbell	Frakes Engineering	Vice President/General Manager	Full Time	Advisory
Douglas Rapp	Cyber Leadership Alliance	President	Full Time	Advisory
Valita Fredland	Indiana Health Information Exchange	Vice President – General Counsel and Privacy Officer	Full Time	Advisory
Frank Nevers	Federal Home Loan Bank of Indianapolis	Information Security Program Manager	Full Time	Advisory
Leon Ravenna	KAR Auction Services	CISO	Full Time	Advisory
Kim Milford	Indiana University	Lead REN-ISAC	Full Time	Advisory
Paul Baltzell	Mainstreet	VP Information Technology Solutions	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - We conducted interviews with three people and summarized questions and findings from the Indiana Medical Device Manufacturer's Council (IMDMC) annual meeting, and two discussions with government officials.
    - Jim Routh, Chief Information Security Officer (CISO), Aetna, board member of National Health Information Sharing and Analysis Center (NH-ISAC), and Financial Services Information Sharing and Analysis Center (FS-ISAC) member.
    - Suzanne Schwartz, Doctor of Medicine (MD), Master of Business Administration (MBA), Director, Medical Device Security, U.S. Food and Drug Administration (FDA)
    - Jennings Aske, Juris Doctor (JD), CISO, Columbia/New York Presbyterian Health.
    - Ralph Hall, Leavitt Partners. We spoke with him and summarized findings from the IMDMC annual meeting, including discussions from Eli Lilly, Roche, Hill-Rom, and the Mako Group. Mitch Parker chaired the Cybersecurity panel with members of Lilly, Hill-Rom, Mako Group, and Dr. Schwartz and gave all research notes to the group.
    - Deven McGraw, Former Deputy Director of Enforcement, U.S. Department of Health and Human Services (HHS) Office For Civil Rights.
    - Iliana Peters, Acting Deputy Director of Enforcement, HHS Office For Civil Rights.
    - Nebraska Hospital Association.
    - Josh Singletary, NH-ISAC.
  - We have also utilized several papers and presentations from Mitch Parker and IU Health to provide further research. The papers supplied have 100+ sources each and were submitted as part of graduate school programs.

- **Research Findings**
  - There is high awareness of cybersecurity being an issue in the State of Indiana and nationally.
  - There has been very little practical guidance given to providers that they can use. While HHS has started to give guidance, there is little practical guidance that applies to small to medium size providers.
  - Currently, in Washington, the Health Information Trust Alliance (HITRUST), a private organization, is actively attempting to usurp the NH-ISAC to be the provider of threat intelligence and reporting to healthcare organizations in the U.S.
    - Many providers will not adopt this framework as it is costly and requires full-time investment to be successful.
      - Full HITRUST adoption also requires vendors to buy into it and use the framework.

        - Lessons learned from Department of Defense (DOD). Special frameworks did not work for them (Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)), and organizations end up falling back to using National Institute of Standards and Technology (NIST) as it is practical and what the rest of the federal government has standardized upon.
- The NH-ISAC is providing all providers with information; however, it is overly technical in nature.
    - While NH-ISAC does have the Threat Intelligence Committee, which is composed of members from the larger providers, and does provide intelligence to other members, it is highly technical in nature most of the time.
- According to the Nebraska Hospital Association, 75% of their hospitals are in rural areas and do not have full-time IT staff.
- According to the American Hospital Association, in 2012, approximately 25% of all hospitals had negative operating margins. The average operating margin was 7.04% for the same time period.
- Electronic Medical Records (EMR) systems require significant initial and ongoing investments. The core EMR system, when purchased initially, requires 25% of the lifetime costs paid up front.
- Even with cloud computing, organizations are required to complete information security risk assessments and document them yearly.
    - There has been a growing perception in healthcare that certain systems that contain protected health information do not need involvement from the formal Info Services e.g. security. This is because the system specific "shadow IT" ends up not waiting for security, doing work, and negating the required security controls necessary to keep them protected.
- Organizations are required, as per the Health Information Technology for Economic and Clinical Health (HITECH) Act, to complete risk assessments of vendors.
- Healthcare organizations are dealing with lower margins, not enough IT staff, and a lack of cohesive guidance.
    - The number of vendor risk assessments that medical device manufacturers have to deal with and the high variety are causing issues with vendors. Jennings Aske is leading an effort to standardize this.
    - While NH-ISAC has the Cyberfit program, which focuses only on applications, licensed by Prevalent, is also costly at $4,000 per assessment. With the number of vendors and applications that a health system can have, if used extensively the program can cost more than staff. Smaller providers typically use the Cyberfit program for a few applications. However, according to Iliana Peters, smaller providers still have to conduct their own organizational risk assessments, even if they do risk assessments of applications.
- The FDA is expecting organizations to include security in their legal contracts. These need to be shared to set global expectations.

- The FDA understands that current medical device security efforts are losing people over unclear explanations and not listening to customers.
- According to the FDA, vendors need to be educated on how to present security. Many of the smaller startups are more willing to listen to customers and present a better security plan to their customers. According to Jennings Aske, some large vendors know how to communicate about their own solutions, while many others do not.
    - Standardization and information sharing in this area would provide benefits, according to Jennings, as vendors would be more willing to work with collaborative groups. Binding together groups of organizations, with aggregate market value commensurate with the size of larger medical device companies, is considered incentive enough, indicates Jennings.
- While researching metrics, the metrics published did not either refer to Bureau of Labor Statistics data on the workforce or only referred to cybersecurity as part of an overall percentage. There is very little empirical data on staffing metrics for cybersecurity as either a subset of IT or healthcare. Only surveys published by Big 4 firms indicate a relative increase in positions, as opposed to a metrics-based approach relative to either organizational size, number of assets managed, or number of applications. The only metrics found specifically related to the number of data breaches themselves.
- According to Jim Routh, Midwestern organizations are less likely to take advice from national organizations. He spent six years as a CISO in Minnesota and made this observation.
- The NH-ISAC will be offering discounted endpoint security for all healthcare providers at a very reasonable cost of $10 per machine per year. This addresses a critical need and costs significantly less than other solutions.
- A number of smaller providers are willing to collaborate. However, not all health systems in Indiana have their security managed locally. St. Vincents, which is part of Ascension, has security managed by an operations center in Troy, Michigan. The issue of collaboration across state lines has to be addressed.
- According to our research, the practical approaches to implementing cybersecurity need to be communicated better to the medical provider community in a way they can use.

- **Committee Deliverables**
    - Vendor Management
    - Long-Term Education
    - Indiana Threat Intelligence Distribution System

- **Additional Notes**
    - The scope of what we researched indicates that there is a gap between education and practical approaches.

- **References**
  - IU Health Business Associate Agreement and Security Exhibit
  - Interview Notes with Jim Routh, CISO, Aetna, and Suzanne Schwartz, MD, MBA, of the FDA – October 2017
  - *Implementing Secure Cloud Computing in Small to Medium Sized Healthcare Environment*
  - Interview/meeting notes from Indiana Medical Device Manufacturer's Council Meeting - November 2017
  - *Improving Healthcare Provider Information Security Through the Implementation of Financial Systems Structures and Controls*

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Centers for Medicare and Medicaid Services (CMS) has released several guidance documents and programs on cybersecurity.
    b. The Healthcare Information and Management Systems Society (HIMSS) currently offers a comprehensive cybersecurity education program, as does the American Hospital Association (AHA), and American Health Information Management Association (AHIMA). In addition, the National Health Information Sharing and Advisory Center (NH-ISAC) and InfraGard also offers guidance to organizations. HITRUST, which is a for-profit organization, is also popular with many large health systems and payers. They have been providing guidance and a security framework.
    c. Much of this education is focused on either the basics or is aimed at highly sophisticated organizations, which is not the majority of healthcare.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Currently, we believe those to be the continuing maintenance and upgrading of systems to protect against new and emerging threats, the abundance of legacy systems, the continuing issues with workflows, the lack of consistent training and education, and the economic pressures causing a de-emphasis on cyber due to having to keep the lights on in many organizations.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. The need to provide basic education that is relevant to organizations to show them how to protect, as opposed to the constant emphasis on data breaches. CMS has directly indicated that education has been a weak point, and our research shows that the current approach of having one dedicated subject matter expert in each regional office isolates security responsibilities to that one person. Whereas, the institutionalization of security standards that the Federal Financial Institutions Examination Council (FFIEC) has accomplished in finance, is a much more comprehensive cybersecurity program model.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. We are required to follow the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, HITECH Act, Stark Act, and a number of state and local laws. In addition, the organizations that have not outsourced their payment processing have to follow Payment Card Industry – Data Security Standards. The organizations that also actively recruit international patients from the European Union (EU) or advertise in the EU must follow the EU General Data Protection Regulation (GDPR).

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. We have highlighted the NH-ISAC Threat Intelligence Committees (TIC) and Cyberfit programs as great examples as for how multiple organizations can work together to identify, classify, and mitigate threats across a large population. We have also discussed how organizations are already self-organizing, specifically with Jennings Aske's work at Columbia/New York-Presbyterian (NYP).

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. We have included two papers written by Mitch Parker, and interviews with Jim Routh, CSO of Aetna; Suzanne Schwartz, MD, MBA, Director of Medical Device Security for the FDA; Ralph Hall from Leavitt Partners at the Indiana Medical Device Manufacturer's Council annual meeting; and Jennings Aske, CISO of Columbia/NYP Health System in New York City (NYC). We have also researched NH-ISAC, Research Education Networking Information Sharing and Analysis Center (REN-ISAC), and a number of other sources.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. They are currently utilizing the same sources we are and also self-organizing as part of emergency management to address these issues. This self-organization includes working with NH-ISAC, REN-ISAC, InfraGard, and through contacts in hospital emergency management, including existing regional organizations.

8. **What does success look like for your area in one year, three years, and five years?**
    a. One year – Begin developing a pilot program modeled after NH-ISAC's Threat Intelligence Committees (TICs) to collaborate across multiple institutions to address security issues, and provide a means for healthcare organizations to contact us to report potential issues. Beginnings of a communication plan designed to reach out to healthcare providers.
    b. Three years – Expansion of the program to have more dedicated staff and interaction with providers. More proactive education. Collaboration with other states and organizations such as NH-ISAC, Infragard, and Department of Homeland Security (DHS) to provide cybersecurity awareness.
    c. Five Years – Having this program as part of normal business of the State.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. There needs to be a concerted effort to reach out to specific medical providers to specifically address what they need to do to increase security. People are very aware of the need for cybersecurity. The specific guidance that they need to be secure has been either too specific or lacking.

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. According to the 2015 U.S. Bureau of Labor Statistics (BLS) statistics, 9.0% of the total workforce in Indiana is in the healthcare sector.
b. There are no clear statistics as to how much of that section workforce is cybersecurity related.
c. IU Health employs approximately 30,000 people. Approximately 550 of which work in IT, which is approximately 2% of the workforce. Of that, 20 staff members are dedicated to cybersecurity full-time, which is approximately 0.07% of the total workforce at IU Health.
d. According to a Frost & Sullivan report, 30% of healthcare hiring managers plan to increase staff by 20% or more, and 9% of managers want to increase hire between 16-20%.
e. According to the May 2017 HealthCare Industry Cybersecurity Task Force report, coupled with the statistics from the BLS 2016-2026 report. The Cybersecurity vacancies for Indiana Healthcare would be around one dedicated Cybersecurity professional for every 10,000 staff with a minim of one.
f. The issue is not cybersecurity jobs, it is getting people to understand cybersecurity and use due diligence.

11. What do we need to do to attract cyber companies to Indiana?

a. Advertise and leverage the educational advantage that Indiana has with IU, Purdue, IUPUI, Rose-Hulman, and Notre Dame. Two of the best and most well-connected Cyber programs in the country are here, and there are already a number of tech companies, specifically Salesforce, taking advantage of that. Facilitating business development and encouraging companies to locate offices and/or staff here based on the availability of top-level graduates, quality of living, and low cost of living would really help.

12. What are your communication protocols in a cyber emergency?

a. We follow the Hospital Incident Command System (HICS) to escalate incidents. We now have coordinated communication with multiple agencies and will follow the same protocols as a standard multi-site incident. Ultimately, a multidisciplinary approach in healthcare is needed that utilizes HICS as patient safety has to be paramount.

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. Focus on assessing risk and helping people understand what to do to address it. The issue is that we do not focus on the fundamentals and need to treat cybersecurity as part of the business, not just something to address separately. The more we focus on it as a separate discipline, the less we will be able to attack root causes for many of these issues.

Deliverable: Vendor Management

Deliverable: Vendor Management

General Information

1. **What is the deliverable?**
    a. Indiana-focused versions of security education targeted at small to medium-sized providers. Most of the guidance given out by CMS to providers makes the assumption that providers either have an IT staff or someone with the requisite level of expertise within the organization to interpret guidance and give the staff an answer. As part of discovery on several other projects, we discovered that most small to medium sized providers and critical access hospitals do not have the staff needed to implement solutions, and that they have not been educated on what to do.
    b. The goal of this solution is to provide staff at small to medium-sized businesses with the information they need to assess and address risk with their third-party vendors that provide services to the healthcare community. In addition, this will provide education that non-technical staff can use to make better purchasing decisions that improve cybersecurity.

2. **What is the status of this deliverable?**
    a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Providers will be able to make better decisions regarding the security and safety of the products they use and maintain at their organization

6. **What metric or measurement will be used to define success?**
    a. Number of providers utilizing the training.
    b. Number of products purchased/evaluated using these guidelines.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Small to medium healthcare entities across the State who do not currently receive this type of information or training on purchasing products.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This partially overlaps with the work NH-ISAC, REN-ISAC, and Infragard are currently doing. However, they are not reaching the smaller providers or providing targeted training toward the purchasing process.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Infragard, NH-ISAC, REN-ISAC, and the State and Local Government committees. We also plan on working with and sharing this information with other committees.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Infragard, NH-ISAC, REN-ISAC, Indiana Office of Technology (IOT), Indiana Hospital Association (IHA).

12. **Who should be main lead of this deliverable?**
    a. Mitch Parker

13. **What are the expected challenges to completing this deliverable?**
    a. Backlash from vendors who will view this as losing sales.
    b. Communicating this out to the right staff that need to see it.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Webinar	Mitch Parker	10	January 2019	Need a platform to host on for everyone – based off of IU Health training
Indiana Medical Device Manufacturer's Council	Mitch Parker	50	November 2018	Conference Organizer has approved in light of June meeting being cancelled for annual meeting.
October 23 Conference	Mitch Parker	10	October 2018	Will need conference organizers to approve
One-pager documents and materials	Mitch Parker and IECC Healthcare Committee	20	February 2019	Two-factor authentication documents awaiting final review, encryption to be done by this date.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0.5	0.5	Marketing / Communications	Indiana IOT	Grant	Need to have someone help with communication and distribution under proper branding

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Webinar Platform	Need to effectively communicate out using IOT approved one			IOT	Grant	We do not have data on Indiana state pricing for these services.
Print/web communications	Need to get the message out to stakeholders.					We do not have data on Indiana state pricing for these services.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The greatest benefit is being able to reach a number of medical device manufacturers in one place and communicate out requirements. In addition, reaching a large number of providers through communications will also help get the message out about vendor management and improving security.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. We will set expectations with the vendors, many of which are headquartered in Indiana, and are reaching specific market segments that up until last year had been underserved in security communication, specifically the orthopedic device manufacturers. We estimated 0.5 of a full-time IOT employee to address facilitating and managing the communication process, and additional communication/marketing costs for webinars and one-pagers.
b. Providers will be able to make better decisions regarding the security and safety of the products they use and maintain at their organization

19. What is the risk or cost of not completing this deliverable?

a. We will not be able to communicate out security and vendor management information to the providers that need it the most in Indiana.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Number of providers utilizing the training.
b. Number of products purchased/evaluated using these guidelines.
c. The baseline will be the number of providers we communicate during the month of August 2018.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. There may be backlash from vendors who could see this as negatively impacting sales.
b. There may be backlash from vendors who see this as potential government infringement on their products.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. We documented that there will be program management/marketing/communications support needed from the State if we are to succeed in this endeavor.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. We have spoken with Infragard, NH-ISAC, REN-ISAC, the Indiana Hospital Association, OrthoWorx, and Indiana University (IU).

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. State and Local Government, Water/Wastewater, Cyber Sharing, and whoever else wants to use it.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. We need to notify all medical device manufacturers in the State, and we can use relationships with the Indiana Medical Device Manufacturer's Council to do so. We have reached out to Tory Castor, SVP Government Affairs at IU Health, to help facilitate. We are already speaking with IU and OrthoWorx Indiana.
b. We would also want to use the communication channels available from IOT and the State under their plan and branding.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. We want to keep the brand and messaging tight and consistent across deliverables. Our greatest concern is that there will be mixed messages across the different committees, and we cannot afford to waste time or give an incoherent message to communities that have little time to waste. We need to be coordinated in this effort and that is where we could have the greatest issue.

Evaluation Methodology

Objective 1: Create vendor management resources for healthcare providers by February 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Distribute vendor management resources to eighty percent of healthcare providers by April 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Long-Term Education

Deliverable: Long-Term Education

General Information

1. **What is the deliverable?**
    a. Indiana-focused versions of security education targeted at small to medium-sized providers. Most of the guidance given out by CMS to providers makes the assumption that providers either have an IT staff or someone with the requisite level of expertise within the organization to interpret guidance and give staff an answer. While working on several other projects, we discovered that most small to medium sized providers and critical access hospitals do not have the staff needed to implement solutions and that they have not been educated on what to do. Most importantly, they do not even know where to report breaches.
    b. The goal of this solution is to give actionable items to these organizations to implement reasonable security solutions and help prevent common security issues with basic targeted education. We have spoken with the Water committee and discovered we had the same issue where most small to medium-sized organizations do not have security staff needed to implement solutions, lacking/no security education, and don't know how to handle breaches.

2. **What is the status of this deliverable?**
    a. In progress; 40% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Providers at all levels will be able to utilize actionable information to protect themselves against emerging threats.
    b. Better community awareness of threats and, more importantly, actionable steps that providers can take to protect themselves using communications they can understand.

6. **What metric or measurement will be used to define success?**
    a. Number of providers utilizing the service and actively protecting themselves.
    b. Number of organizations receiving intelligence (time period comparisons).

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Small to medium healthcare entities across the state who do not currently receive this type of actionable intelligence.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This currently partially overlaps with the work NH-ISAC, REN-ISAC, and InfraGard are currently doing. However, they are not reaching to the level we intend to.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. InfraGard, NH-ISAC, REN-ISAC, and the State and Local Government committees. We also will hopefully be working with the Water committee as we share the same challenges.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. InfraGard, NH-ISAC, REN-ISAC, Indiana IOT, Indiana Hospital Association, Indiana Health Information Exchange (IHIE).

12. **Who should be main lead of this deliverable?**
    a. Mitch Parker

13. **What are the expected challenges to completing this deliverable?**
    a. Communicating to the providers and utilizing multiple avenues to do so.
    b. Threat Complexity. Having to deal with multiple threat variants affecting providers.
    c. Bad patches from vendors (Meltdown/Spectre). Red Hat, Microsoft, and numerous other vendors have released bad patches for vulnerabilities. We don't want to cause machines to malfunction because of non-functional patches.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Educational Programs	Mitch Parker and IECC Healthcare Committee	50	March 2019	Will be using previously developed content
Webinars	Mitch Parker	50	February 2019	Will be using previously developed content
One-pager documents	Mitch Parker and IECC Healthcare Committee	20	February 2019	Encryption and one other document to be ready by then

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0.5	0.5	Marketing / Communications	IOT	Grant	Need to have someone help with communication and distribution under proper branding

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Webinar Platform	Need to effectively communicate out using IOT approved one			IOT	Grant	We do not have data on Indiana state pricing for these services.
Print/web communications	Need to get the message out to stakeholders.					We do not have data on Indiana state pricing for these services.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. We will be able to reach an underserved population that traditionally has been ignored by cybersecurity efforts and provide them with information they can use.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will reduce risk and impact by providing targeted communications to a population that historically has not received them. The costs would include a full-time or equivalent FTE to own the program at the IOT level, resources needed for communication (email, website, postal mailings), and the time from committee member institutions needed to craft the messaging. Enforcement will be through the committee chairs and designates working to allocate resources and monitoring contributions.

19. What is the risk or cost of not completing this deliverable?

a. We will continue to have cybersecurity and ransomware attacks that can be easily preventable affecting both patients and providers in this State. Indiana has made national headlines for several ransomware attacks. We need to prevent the numerous small businesses and providers that make up the bulk of our healthcare providers from falling victim to similar attacks.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Number of providers utilizing the service and actively protecting themselves.
b. Number of organizations receiving intelligence (time period comparisons).
c. We are going to use the number of providers using these in August 2018 as the baseline.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The largest factor would be the necessity of having someone in IOT in place to facilitate getting us this list.
b. The other major factor is making sure we have enough coverage from members to address covering the news and intelligence sources to develop communications.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. We will need a resource within IOT who can work on behalf of the committee coordinating it and making sure information is current.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Chetrice Mosley.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors:**
    i. Water/Wastewater, Cyber Sharing, and State/Local Government.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. We believe that all other sectors should be informed as we want them to use it as well.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. We should discuss unifying this with other communications that IOT and other agencies put out so that we give a consistent message to constituents.

Evaluation Methodology

Objective 1: IECC Healthcare Committee will create Indiana-focused versions of security education by March 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Provide Indiana-focused versions of security education to eighty percent of Indiana healthcare providers by May 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Indiana Threat Intelligence Distribution System

Deliverable: Indiana Threat Intelligence Distribution System

General Information

1. **What is the deliverable?**
    a. An Indiana-focused version of the NH-ISAC Threat Intelligence Committee focused on distributing information to all levels of providers. Based on conversations with several NH-ISAC representatives, as well as representatives from several other organizations, the major issue is that people are aware of threats, but not how to respond to them.
    b. This deliverable would be representatives of larger health systems taking threat intelligence from NH-ISAC, REN-ISAC, and numerous other sources, and providing actionable information that small to medium size providers can use as a checklist to ensure they are protected against vulnerabilities rather than the current system where providers have to interpret the threats themselves.
    c. The current efforts, while valiant, are representative of the issue that internal security services needs to better communicate with other organizations and within the organizations that they belong to.

2. **What is the status of this deliverable?**
    a. Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Providers at all levels will be able to utilize actionable information to protect themselves against emerging threats.
    b. Better community awareness of threats, and more importantly, actionable steps that providers can take to protect themselves using communications they can understand.

6. **What metric or measurement will be used to define success?**
    a. Number of providers utilizing the service and actively protecting themselves.
    b. Number of organizations receiving intelligence (time period comparisons).

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Small to medium healthcare entities across the state who do not currently receive this type of actionable intelligence.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This currently partially overlaps with the work NH-ISAC, REN-ISAC, and InfraGard are currently doing. However, they are not reaching to the level we intend to.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. InfraGard, NH-ISAC, REN-ISAC, and the State and Local Government committees.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. InfraGard, NH-ISAC, REN-ISAC, IOT, Indiana Hospital Association, Indiana Health Information Exchange.

12. **Who should be main lead of this deliverable?**
    a. Mitch Parker

13. **What are the expected challenges to completing this deliverable?**
    a. Communicating to the providers and utilizing multiple avenues to do so.
    b. Threat Complexity. Having to deal with multiple threat variants affecting providers.
    c. Bad patches from vendors (Meltdown/Spectre). Red Hat, Microsoft, and numerous other vendors have released bad patches for vulnerabilities. We don't want to cause machines to malfunction because of non-functional patches.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Identify Medical Providers and Healthcare Organizations	IOT/Professional Licensing Agency/State DOH	0	October 2018	We need to have this hosted by IOT or the state government.
Identify participating healthcare organizations	Mitch Parker, Jake Butler	0	October 2018	
Develop Communication Strategy	Mitch Parker, Jake Butler, Frank Nevers	0	October 2018	
Develop initial pilot group	Andy VanZee, Mitch Parker	0	November 2018	
Send initial messages	Mitch Parker, Jake Butler	0	December 2018	
Gather feedback and refine	Team	0	February 2019	
Continue to send messages	Team	0	February 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1	1	Security/Threat Intelligence	IOT	Grant	We need to have a resource within state government/IOT able to own the program and sustain it on behalf of the committee and maintain web site
0.25	0.25	Provider-side threat intelligence	Participating healthcare providers		We need resources at the providers who can distill this intelligence and craft communications for end users/providers.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Email address	Need a group email to send communications out to			IOT		
Web Site	Need to have a web site to communicate out					
Marketing/Mailing Lists	Need to send initial communications and ongoing large-scale alerts out to providers					

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Utilizing the resources of the Indiana state government, specifically the Professional Licensing Agency and Department of Health, current medical and healthcare providers can be identified and targeted for specific cyber education. Current efforts alert people there is an issue, but do not provide targeted remediation guidance. The resources of the Indiana state government can be utilized to address a critically underserved group that is not communicated to. As these providers have to register with the State to stay current, we will be able to utilize the maintained lists to target a current group.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will reduce risk and impact by providing targeted communications to a population that historically has not received them. The costs would include a full-time or equivalent FTE to own the program at the IOT level, resources needed for communication (email, website, postal mailings), and the time from committee member institutions needed to craft them.

19. What is the risk or cost of not completing this deliverable?

a. We will continue to have cybersecurity and ransomware attacks that can be easily preventable affecting both patients and providers in this State. Indiana has made national headlines for several ransomware attacks. We need to prevent the numerous small businesses and providers that make up the bulk of our healthcare providers from falling victim to similar attacks.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Number of providers utilizing the service and actively protecting themselves.
b. Number of organizations receiving intelligence (time period comparisons).
c. The baselines will be the groups signed up or communicated to in August 2018.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The largest factor would be the necessity of having someone in IOT in place to facilitate getting us this list.
b. The other major factor is making sure we have enough coverage from members to address covering the news and intelligence sources to develop communications.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. We will need a resource within IOT who can work on behalf of the committee coordinating it and making sure information is current.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Chetrice Mosley.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. Water/Wastewater, Cyber Sharing, and State/Local Government

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. We need to notify the other committees, IOT, and the providers listed. Resources included in the plan for initial mailings and communications.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. We want to make sure that this is being covered under the right branding, and that we work with Indiana state marketing agencies and resources to develop clear and consistent communications.

Evaluation Methodology

Objective 1: Develop a pilot program with three participants of the Indiana Health Cyber Threat Intel Committee by November 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Evaluate pilot program and recommend a sustainability framework model for the state of Indiana to maintain by February 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- IECC Healthcare Committee Jim Routh Meeting Notes
- IECC Healthcare Committee Indiana Medical Device Manufacturers Council (IMDMC) Meeting Notes
- IU Health Business Associate Agreement and Security Exhibit
- Lasalle University Implementing Secure Cloud Computing in the Small to Medium-Sized Healthcare Environment
- Temple University Improving Healthcare Provider Information Security Through the Implementation of Financial Systems Structures and Controls

IECC Healthcare Committee

Jim Routh Meeting Notes

October 2017

Jim Routh and Dr. Suzanne Schwartz writeup

10/30/2017

Jim Routh – Aetna CISO -

Questions:

1. What have you found effective with information sharing in FS-ISAC?
    1. NH-ISAC?

The key here has been the Threat Intelligence Committees, TICs, which are made up of the best malware hunters and threat analysts across the member organizations, do the initial triaging and make the determination as to what information to distribute. They specifically look to see if these attacks are targeted, or if they are opportunistic. They then make specific recommendations as to actions to take to protect organizations. It is important to note that these are member organizations.

The TICs help out smaller organizations by giving them specific guidance. This is better for smaller organizations that have 1-2 IT people total.

What has been effective in both the NH and FS-ISAC committees is that they give targeted advice to smaller providers. Many of the NH-ISAC programs, such as Cyberfit, are geared toward smaller providers.

2. What areas have you found for improvement in FS-ISAC and NH-ISAC?

The membership has been growing at 30-40 members a month. However, the issue has been getting members. The major issue has been that HITRUST has been lobbying Congress to be the framework and vehicle of choice for dissemination of threat intelligence. HITRUST is a for-profit corporation attempting to push a framework which many small providers will not adapt. NH-ISAC, on the other hand, is non-profit and is a collaborative of many of the largest health systems modeled after FS-ISAC.

FS-ISAC has significant governmental support, including the states of NY and MA, which mandate membership. NH-ISAC has not gotten the level of support it needs because HITRUST has been lobbying against it to Congress, specifically the House Energy and Commerce Committee.

NH-ISAC is also attempting to provide for smaller medical providers by signing a joint partnership agreement with a next-generation endpoint protection company. This will allow them to provide endpoint protection at approx. $10/computer per year, and is aimed at smaller providers with less than 200 total seats. This is significantly less than other solutions, specifically Microsoft's.

Specifically, the area for improvement is to get organizations to adopt NH-ISAC's information sharing and protection plans, and see the benefit, rather than the intense lobbying effort from HITRUST which is damaging NH-ISAC.

Collaboration is absolutely key. People in the Midwest aren't going to listen to a national organization. They're going to want to collaborate with themselves first. Jim is a former Minnesota resident who worked there for 6 years, which is why he made that statement.

While we have NH-ISAC, the best conduit is going to be Indiana itself.

3. What do you think makes up a good education program?

People are well aware of what cybersecurity is now. They need to know what to do and how to act, and your training needs to focus on that rather than just more awareness. We have the awareness part down. People need to know what to do!

4. How do you best structure security programs to accommodate a high variety of scale?

This is where you have to leverage the ISACs to provide this information and use them to help with distribution

5. Anything else?

We've found that the use of DMARC, which is very simple to set up in Office365, but not in Google, is very effective at stopping Phishing attacks.

You also need to remove the use of the SSN wherever not absolutely necessary. Aetna has cleaned up over 7 billion SSNs and still has 2 years to go on the project. This is a long-term commitment companies need to make.

Bonus – Dr. Suzanne Schwartz – FDA

I interviewed her as part of the Indiana Medical Device Manufacturer's Council panel I am moderating on Nov. 1.

Advice from her:

1. Collaboration is key, especially with medical devices.
2. Cannot address this in a siloed manner at all.
3. There needs to be a balance. You need to pause and listen when presenting, and read the audience. People get lost with acronyms and without explanations.
4. Current medical device security efforts are losing people over unclear explanations and not listening.
5. We need to be proactive and address issues right then and there.
6. We need to have this information in contracts. Those need to be shared to set global expectations.
7. Vendors need to be educated. Some big companies get it, many don't. Many of the smaller startups are more willing to listen.
8. There needs to be two-way dialogue between the vendors and customers to set the right level of expectations.

IECC Healthcare Committee

Indiana Medical Device Manufacturers Council (IMDMC) Meeting Notes

November 2017

Notes from IMDMC Meeting:

1. I spoke with Ralph Hall, Partner, Leavitt Partners. He is friends with our General Counsel, Mary Beth Claus, and worked with her for a number of years.
2. Ralph has indicated that there is a lack of federal standards for medical device cybersecurity.
3. The current congressional gridlock has caused any meaningful legislation to have no chance.
4. Medical device manufacturers, due to the lack of federal standards, are trying to rely on state standards.
5. At this point there are upwards of 20, and the companies are having a very difficult time keeping up. There is no agreement on what standards to follow.
6. From me, not Ralph - The EU is doing a better job with GDPR, and may end up being the de facto standard with ISO in light of the current situation.
7. Medical Device Vendors are developing their own standards and are willing to work with companies on them. They are cooperating. Best examples I can give are the collaboration between Merck and Eli Lilly, and the current proposed research collaboration of IU/IU Health/Eli Lilly/Cisco we are working with Von Welch on. I can also give the examples of BD and IU Health, and GE Healthcare and IU Health.
8. NH-ISAC is ineffective at best. Despite the best efforts of Jim Routh, the information they give out is often duplicative and does not show true direction.
9. If we do this, we need to do it ourselves. However, this does not solve for the other 49 states. If we do this, we may do this and set a true example for others.
10. We can take advantage of what NH-ISAC has to offer, but we need to make this accessible for Hoosiers.

IU Health

Business Associate Agreement and Security Exhibit

February 2017

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA"), by and between _____ ("Business Associate"), of _____, and _____ and Indiana University Health, Inc. (individually and collectively referred to herein "Covered Entity"), of _____ Indiana, _____ is made and effective conterminously with the parties' service agreement ("Service Agreement"), to which it is attached.

RECITALS

WHEREAS, Business Associate agrees to provide certain services ("Services") for or on behalf of Covered Entity in accordance with the parties' Service Agreement; and

WHEREAS, in connection with those Services, Covered Entity plans to disclose to Business Associate certain Protected Health Information ("PHI" – used to refer specifically to data controlled or owned by Covered Entity), including electronic PHI or ePHI, (as defined in 45 C.F.R. §160.103) that is subject to protection under the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191 ("HIPAA") Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule", 45 C.F.R. Parts 160 and 162 and Part 164, Subparts A and E); and 45 C.F.R. Parts 160 and 162 and Part 164, Subparts A and C, the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule"); Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), also known as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law No. 111-005 ("ARRA"); and 45 CFR Parts 160 and 164 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule - all together, as amended from time to time, herein referred to as the "Privacy and Security Rules"; and

WHEREAS, Covered Entity and Business Associate acknowledge that each has obligations in its respective role as Covered Entity and Business Associate under the Privacy and Security Rules, as well as regulations promulgated thereunder; and

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI accessed by or disclosed to Business Associate pursuant to their Service Agreement in compliance with this BAA and the Privacy and Security Rules; and

WHEREAS, the purpose of this BAA is to satisfy certain standards and requirements of the Privacy and Security Rules, including the requirement of an appropriate agreement between Covered Entity and Business Associate that meets the applicable requirements of the Privacy and Security Rules.

NOW THEREFORE, in consideration of the mutual promises and covenants, herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. **Definitions.**

   Capitalized terms used in this BAA and not otherwise defined herein shall have the same meanings set forth in the Privacy and Security Rules which definitions are incorporated in this BAA by this reference.

2. **Permitted Uses and Disclosures by Business Associate.**

   a. *Performance of Services.* Except as otherwise limited in this BAA, Business Associate may only use or disclose PHI to perform the services set forth in the Service Agreement, as permitted or required by this BAA, or as Required by Law. Business Associate agrees to limit its uses, disclosures and requests for PHI to the minimum amount necessary to perform its obligations.

   b. *Proper Management and Administration*. Except as otherwise limited in this BAA, Business Associate may use or disclose PHI as necessary for Business Associate's proper management and administration or to fulfill its legal responsibilities, provided that: (1) the disclosures are Required by Law, or (2) Business Associate obtains reasonable assurances from the third party to whom the PHI is disclosed in the form of a written agreement with terms similar to and consistent with this BAA that the PHI will remain confidential and used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the third party, and the third party notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

   c. *Data Aggregation.* Except as the parties might otherwise agree in writing, Business Associate shall only provide data aggregation services on Covered Entity's behalf if specifically directed to do so in writing.

   d. *De-Identified Information.* Business Associate may create, use and disclose de-identified information if required for purposes of providing Services. Business Associate shall not use Covered Entity's de-identified information for its own purposes, except on a case by case basis with Covered Entity's separate prior written agreement for a proposed use. De-identification must comply with 45 CFR §164.502(d), and any such de-identified information must meet the standard and implementation specifications for de-identification under 45 CFR §164.514(a) and (b), or as they may be amended from time to time.

3. **Prohibition on Certain Uses and Disclosures and Compliance with Transaction Standards.**

   a. *As Permitted in this BAA.* Business Associate shall not use or disclose Covered Entity's PHI other than as permitted or required by this BAA or as Required by Law. This BAA does not authorize the Business Associate to request, use, disclose, maintain or transmit PHI in any manner that violates the Privacy and Security Rules if done by Covered Entity.

   b. *Electronic Transactions*. Business Associate hereby represents and warrants that to the extent it is transmitting any HIPAA Transactions for Covered Entity, the format and structure of such transmissions shall be in compliance with the Transaction Standards provided that it is Covered Entity's responsibility to ensure that appropriate Code Sets are used in the coding of services and supplies. Business Associate shall indemnify and hold Covered Entity harmless from any monetary penalties assessed against Covered Entity arising from a breach of the representation and warranty contained herein, including reimbursing Covered Entity for any cost incurred by Covered Entity as a result of an audit or investigation by the Secretary which may include the costs of consultants and lawyers.

4. Compliance with the HITECH Act.

Business Associate shall comply with all additional requirements of the HITECH Act, including, but not limited to:

a. Compliance with the requirements regarding minimum necessary under HITECH § 13405(b);
b. Requests for restrictions on use or disclosure to health plans for payment or health care operations purposes when the provider has been paid out of pocket in full, consistent with HITECH § 13405(a);
c. The prohibition of the sale of PHI without authorization unless an exception exists under HITECH § 13405(d);
d. The prohibition on receiving remuneration for certain communications that fall within the exceptions to the definition of marketing under 45 C.F.R. § 164.501 unless permitted by this BAA and Section 13406 of HITECH;
e. The requirements relating to the provision of access to certain information in electronic format under HITECH § 13405(e);
f. Compliance with each of the Standards and Implementation Specifications of 45 C.F.R. §§ 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards) and 164.316 (Policies and Procedures and Documentation Requirements); and
g. The requirements regarding accounting of certain disclosures of PHI maintained in an Electronic Health Record under HITECH § 13405(c).

5. Safeguards, Subcontractors, Training and Enforcement.

a. *Safeguards.* In accordance with Subpart C of 45 CFR Part 164, Business Associate shall implement and use appropriate and industry best practice technical, procedural and physical safeguards to prevent unauthorized use or disclosure of Covered Entity's PHI, including implementing requirements of the Security Rules with regard to electronic PHI and all applicable laws, regulations and guidance documents. Likewise, Business Associate acknowledges that it is directly liable under the Security Rules and may be subject to civil and, in some cases, criminal penalties for:

   i. failing to safeguard PHI, including electronic PHI, in accordance with the HIPAA Security Rules; and

   ii. uses or disclosures of PHI that are not authorized by this BAA or Required by Law.

   Business Associate shall provide Covered Entity with information concerning the aforementioned safeguards and/or other information security practices as they pertain to the protection of Covered Entity's PHI, as Covered Entity may from time to time request.

b. *Agents/Subcontractors.* In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), before disclosing any PHI received from Covered Entity or created on behalf of Covered Entity, Business Associate will enter into a written agreement with any agents and subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate, and the terms of such agreement shall be at least as stringent as the restrictions and conditions with respect to the use, protection and disclosure of such PHI that that apply to Business Associate pursuant to this BAA. Business Associate will ensure that any agents and subcontractors to whom it provides PHI agree to

implement reasonable and appropriate safeguards to protect such information.

c. *Training*. Business Associate shall provide all of its employees and members of its workforce who will have access to PHI with general HIPAA-related training and education prior to allowing the employees and members of its workforce access to PHI. Such training will be conducted at least annually.

d. *Audit, Inspection and Enforcement*. Business Associate agrees that upon reasonable notice of at least ten (10) business days, Covered Entity may audit the Business Associate's security and privacy policies and procedures, including its security safeguards, to ensure the appropriate protections are in place for Covered Entity's data. Such audit by Covered Entity may be performed by a third party of Covered Entity's choosing and expense to perform compliance analysis of Business Associate's practices with respect to the Privacy and Security Rules, including vulnerability or penetration testing or physical assessments of Business Associate's operations that relate to Covered Entity's PHI. The parties agree to cooperate so that such audits are coordinated to minimize any negative effect on the operation of Business Associate's database, application or systems as a result of such a review. Covered Entity will also provide Business Associate with a copy of the results of such testing. The fact that Covered Entity inspects, or fails to inspect, or has the right to audit or inspect Business Associate's facilities, systems, books, records, agreements, policies and procedures does not relieve Business Associate of its responsibilities to comply with the Service Agreement, this BAA, and applicable HIPAA Regulations, nor does Covered Entity's (i) failure to detect or (ii) failure to notify Business Associate of or to require Business Associate to remedy a detected unsatisfactory practice, constitute an acceptance of such practice by Covered Entity or a waiver of Covered Entity's enforcement rights under the Service Agreement or this BAA. In addition, Business Associate agrees to use good faith efforts to retain the right to audit the privacy and security policies and procedures of its agents and subcontractors who may use or disclose PHI.

e. *Service Organization Control Reports.* Due to the increased security, availability, processing integrity, confidentiality, and privacy risks of using Business Associate to deliver Services to or on behalf of Covered Entity, Business Associate agrees to annually provide a Service Organization Control 2 (SOC 2) Type 2 report to Covered Entity if (1) it provides Service Organization services to Covered Entity involving IU Health Confidential Information that Covered Entity would otherwise perform such as medical record services, data centers, IT managed services, software as a service (SaaS) vendors, and many other technology and cloud-computing based businesses, or (2) it is required as more particularly described in Exhibit A attached hereto. For the purposes of this BAA, IU Health Confidential Information shall mean all non-public information, including, but not limited to, PHI, limited data sets, payment information, personally identifiable information (PII), nonpublic personal information (NPI), Covered Entity proprietary information, sensitive data or information, such that unauthorized access to such data may result in serious financial, legal or operational impact to Covered Entity.

6. Obligation of Business Associate.

a. *Access to Information.* Within ten (10) business days of request from Covered Entity, Business Associate shall make available PHI in a Designated Record Set, to Covered

Entity, as necessary to satisfy Covered Entity's obligations under 45 CFR § 164.524, including providing or sending a copy to a designated third party and providing or sending a copy in electronic format, to the extent that the PHI in Business Associate's possession constitutes a Designated Record Set. Business Associate will not respond directly to an Individual's request for access to their PHI held in the Business Associate's Designated Record Set. Business Associate will direct the Individual to the Covered Entity so that Covered Entity can coordinate and prepare a timely response to the Individual.

b. *Amendment of PHI*. Within ten (10) business days of request from Covered Entity, Business Associate shall make any amendment(s) to PHI in a Designated Record Set, as necessary to satisfy Covered Entity's obligations under 45 CFR § 164.526. Business Associate will not respond directly to an Individual's request for an amendment of his PHI held in the Business Associate's Designated Record Set. Business Associate will direct the Individual to the Covered Entity so that Covered Entity can coordinate and prepare a timely response to the Individual.

c. *Accounting of Disclosures.* Business Associate agrees to document all disclosures of PHI which would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR 164.528. Within ten (10) business days of notice by Covered Entity to Business Associate that Covered Entity has received a request for an accounting of disclosures of PHI, Business Associate shall make available to Covered Entity information to permit Covered Entity to respond to the request. Business Associate will not respond directly to an Individual's request for an accounting of disclosures. Business Associate will direct the Individual to the Covered Entity so that Covered Entity can coordinate and prepare a timely accounting for the Individual.

d. *Remuneration.* Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI as prohibited by 45 CFR § 164.502(a)(5)(ii).

e. *U.S. Department of Health and Human Services*. Business Associate shall make available its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for purposes of determining Covered Entity's compliance with the Privacy and Security Rules. Unless the Secretary directs otherwise or it is otherwise prohibited by law, Business Associate shall promptly notify Covered Entity of Business Associate's receipt of such request, so that Covered Entity can assist in compliance with that request.

f. *Judicial and Administrative Proceedings*. In the event Business Associate receives a subpoena, court or administrative order or other discovery request or official mandate for release of PHI, Business Associate shall notify Covered Entity in writing prior to responding to such request to enable Covered Entity to object. Business Associate shall notify Covered Entity of the request as soon as reasonably practicable, but in any event, within two (2) business days of receipt of such request.

g. *Reporting*. Business Associate shall immediately notify, no later than one (1) business day from discovery of a potential event affecting Covered Entity's data, the designated Chief Privacy Officer of the Covered Entity of: (1) any use or disclosure of PHI by

Business Associate not permitted by this BAA; (2) any Security Incident (*see explanation below)*; (3) any breach of unsecured Protected Health Information as defined in the HITECH Act; or (4) any other security breach of an electronic system, or the like, as such may be defined under applicable state law.

h. *Explanation of Security Incident*. For purposes of this BAA, "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Covered Entity requires prompt notification from Business Associate if Business Associate experiences any Security Incident that compromises the confidentiality, integrity or availability of Covered Entity's data or information systems. Below are some examples of a Security Incident:

1) Business Associate information systems are exposed to malicious code, such as a virus or worm, and such code could be transmitted to Covered Entity's data or systems.

2) Unauthorized access is granted or obtained to servers or workstations that contain Covered Entity's data or Business Associate discovers that Covered Entity's data is being used, copied, or destroyed inappropriately.

3) Business Associate experiences an attack or the compromise of a server or workstation containing Covered Entity's information requiring that it be taken offline.

4) Unauthorized access, use or disclosure has occurred involving Protected Health Information, which is an obligation under the Privacy Rule.

The Parties agree that this section satisfies any notices necessary by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. For purposes of this BAA, "Unsuccessful Security Incidents" include activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of electronic PHI.

i. *Breach.* Within one (1) business day of discovery of a reportable Security Incident as described above or breach of unsecured PHI, Business Associate shall notify Covered Entity of the existence and nature of the incident as understood at that time. Business Associate shall immediately investigate the incident and within ten (10) business days of discovery shall provide to Covered Entity, in writing, a report describing the results of Business Associate's investigation, including:

1) the date of the breach;
2) the date of the discovery of the breach;
3) a description of the types of PHI that were involved;
4) identification of each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and
5) any other details necessary to complete a risk assessment in accordance with the HITECH Act.

Reporting and other communications made to the Covered Entity under this section must be made to the Covered Entity's Chief Privacy Officer at:

Indiana University Health
ATTN: Privacy Counsel Office
340 W. 10th Street
Fairbanks Hall - Suite #3100
Indianapolis, IN 46202
Phone: 317-963-1940
Email: HIPAA@iuhealth.org

Business Associate shall cooperate with Covered Entity in investigating a breach and in meeting Covered Entity's obligations under the HITECH Act, and any other security breach notification laws or regulatory obligations.

Under certain circumstances, as solely directed by the Covered Entity, Business Associate will send or cause notifications to be sent directly to affected Individuals. Business Associate will comply with the requirements pursuant to 45 C.F.R. § 164.404. Prior to sending notification to the affected individuals, Business Associate will provide Covered Entity with an advance copy of the proposed letter for review and approval.

Business Associate shall be responsible for the mandatory reporting of breaches for which Business Associate is responsible to the Office of Civil Rights.

j. *Incident Costs.* In the event of a Breach of Unsecured PHI which Covered entity or other entity with Privacy and Security Rules enforcement jurisdiction determines was proximately caused by Business Associate for which HIPAA requires notice to be provided to individuals pursuant to 45 C.F.R. §§ 164.404 and 164.406, Business Associate shall be responsible for all costs associated with the incident, including but not limited to: (i) costs to print and mail the notification letters to affected individuals; (ii) media notification costs to the extent such media notification is required by applicable law; (iii) costs for Business Associate to set up a call center if Business Associate reasonably determines that such is necessary to handle inquiries; and (iv) credit monitoring costs if Covered Entity reasonably determines that it is necessary to mitigate harm for affected individuals.

k. *Mitigation.* Business Associate will cooperate with Covered Entity's efforts to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate not provided for in the Service Agreement or this BAA or that is not in accordance with HIPAA and the HITECH Act or other applicable law.

l. *Notice of Privacy Practices.* Business Associate will abide by the limitations of any Notice of Privacy Practices ("Notice") published by Covered Entity of which Covered Entity provides notice to Business Associate in accordance with the Covered Entity Obligations section of this BAA.

7. Obligations of Covered Entity.

a. *Notification of Changes Regarding Individual Permission.* Covered Entity will notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI. Covered Entity will provide such notice to Business Associate who shall implement the change no later than fifteen (15) business days after

such notice. Covered Entity will obtain any consent or authorization that may be required by the Privacy or Security Rules, or applicable state law, prior to furnishing Business Associate with PHI. If the use or disclosure of PHI in this BAA is based upon an Individual's specific authorization for the use of his PHI, and the Individual revokes such authorization in writing, or the effective date of such authorization has expired, or authorization is found to be defective in any manner that renders it invalid, Business Associate agrees, upon receipt of notice from Covered Entity of such revocation or invalidity, to cease the use and disclosure of any such Individual's PHI except to the extent it has relied on such use or disclosure, or where an exception under the Privacy and Security Rules expressly applies.

b. *Notification of Restrictions to Use or Disclosure of PHI*. Covered Entity will notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522 or 42 U.S.C. § 17935(a), to the extent that such restriction may affect Business Associate's use or disclosure of PHI. If Business Associate reasonably believes that any restriction agreed to by Covered Entity pursuant to this Section may materially impair Business Associate's ability to perform its obligations under the Service Agreement or this BAA, the Parties will mutually agree upon any necessary modification of Business Associate's obligations under such agreements.

8. Insurance and Indemnification.

a. *Insurance*. Business Associate represents and warrants that during the term of the Service Agreement, it shall maintain commercially reasonable and sufficient insurance to adequately underwrite the potential risks associated with the Services, including but not limited to regulatory or administrative investigations or fines and appropriate cybersecurity coverage for privacy and security risks. This includes Business Associate's maintenance of cyber liability insurance with minimum limits of $5 million per occurrence. Upon request, Business Associate shall provide evidence of continuous coverage to Covered Entity and no coverage required within this section shall be voided or cancelled without prior notice to Covered Entity.

b. *Indemnification*. The Parties agree to indemnify, defend and hold harmless each other and each other's respective employees, directors, officers, subcontractors, agents or other members of its workforce, each of the foregoing hereinafter referred to as "indemnified party," against all actual and direct losses suffered by the indemnified party and all liability to third parties arising from or in connection with any breach by the indemnifying party or its employees, directors, officers, subcontractors, agents or other members of its workforce of this BAA or of any warranty hereunder or from any negligence or wrongful acts or omissions, including failure to perform its obligations under the Privacy and Security Rules. Accordingly, on demand, the indemnifying party shall reimburse the indemnified party for any and all actual and direct losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any indemnified party by reason of a suit, claim, action, proceeding, regulatory or administrative investigations or fines, or demand by any third party which results from the indemnifying party's breach hereunder. The Parties' obligation to indemnify any indemnified party shall survive the expiration or termination of this BAA.

9. Term and Termination.

a. *Term.* The term of this BAA shall be conterminous with that of the Service Agreement and shall terminate at the expiration or termination of that Agreement or when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity.

b. *Termination for Breach.* Upon either party's knowledge of a material breach by the other party of this BAA, the non-breaching party will provide written notice to the breaching party detailing the nature of the breach and provide an opportunity for the beach to be cured within thirty (30) business days. Upon expiration of such thirty (30) day cure period, the non-breaching Party may terminate this BAA and, at its election, the Service Agreement, if cure has not been affected or is not possible.

c. *Effect of Termination.* Upon termination of the Service Agreement or this BAA, for any reason, Business Associate shall return or destroy (as directed by Covered Entity) all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate maintains in any form. Business Associate shall retain no copies of the PHI unless otherwise specifically agreed in writing by the parties. Business Associate shall certify in writing to Covered Entity the proper and timely return or destruction of PHI within ten (10) days of the termination of this BAA. If it is not feasible to return or destroy such PHI upon termination of this BAA, then Business Associate shall:

i. so inform Covered Entity, and Business Associate shall extend the protections of this BAA to the PHI and limit any further uses and disclosures;

ii. retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out Business Associates' legal responsibilities;

iii. continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

iv. not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out above which applied prior to termination; and

v. when it becomes feasible, return to Covered Entity or destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities. The terms and conditions of this section shall survive the expiration or termination of the Service Agreement.

For more information on the requirements for destruction of data, please see the Indiana University Health, Inc. Security Requirements in Exhibit A to this BAA.

10. Miscellaneous Provisions.

a. *Security Requirements*. Business Associate shall comply and shall cause its workforce

to comply (to the extent applicable to individuals) with the provisions set forth in Exhibit A (referred to as the "Indiana University Health, Inc. Security Requirements"). As periodically requested by IU Health, but no more frequently than annually, Business Associate shall promptly, fully and accurately complete an IU Health Information Security Questionnaire and other documents or requests for information regarding Business Associate's information security practices.

b. *Continuity of Business*. Business Associate shall ensure that any and all data that it manages on Covered Entity's behalf shall be secured and backed up such that in the event that the Business Associate's services or data center containing Covered Entity's data suffers an adverse system event, Covered Entity shall be able to continue its business as intended with respect to the Services provided by Business Associate to Covered Entity under the Service Agreement. Therefore, Business Associate shall maintain such processes in place to ensure that in the event that it is bankrupt, data is corrupted or other interruption of its services that it has sufficient contingency plans in place to allow Covered Entity to continue its operations using the data it has entrusted to Business Associate.

c. *Notices*. Any notices pertaining to this BAA shall be given in writing and shall be deemed duly given to a Party or a Party's authorized representative identified in the Service Agreement in accordance with the Agreement's notice provision or, if no such provision exists, within three days of having sent the mail via certified USPS mail or via e-mail with electronic return-receipt received.

d. *Privacy and Security Responsible Individuals*. Business Associate shall provide to Covered Entity the contact information for primary individuals responsible for privacy and security compliance for Business Associate's organization. Business Associate agrees to update Covered Entity in the event that the primary responsibility falls to a different individual.

e. *Amendments*. This BAA and attached Exhibit A may not be changed or modified in any manner except by an instrument in writing signed by a duly authorized officer of each of the Parties hereto. The parties acknowledge that the Privacy and Security Rules and the HITECH Act may be modified from time to time. In the event of any such change, both parties agree to immediately enter into good faith negotiations to amend this BAA, through a written document signed by the parties, to conform to any new or revised legislation, rules and regulations to which the parties are subject.

f. *Interpretation*. Any ambiguity in this BAA shall be interpreted to permit the Covered Entity to comply with the Privacy and Security Rules and the HITECH Act.

g. *Geographic Limitations*. Business Associate shall not create, receive, maintain, transmit, use or disclose PHI outside of the United States without the written consent of Covered Entity.

h. *Choice of Law*. This BAA and the rights and the obligations of the Parties hereunder shall be governed by and construed under the laws of the State of Indiana, agreeing not to apply the conflict of laws principles.

i. *Assignment of Rights and Delegation of Duties*. This BAA is binding upon and inures to the benefit of the Parties hereto. Neither Party may assign any of its rights or delegate any of its obligations under this BAA without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed.

j. *Data Ownership*. Unless otherwise specifically set forth in the Service Agreement, Covered Entity owns or controls, and shall continue to own or control, any and all data and PHI shared with Business Associate in order to allow Business Associate to perform its Services under the Service Agreement.

k. *Nature of BAA*. Nothing in this BAA shall be construed to create (i) a partnership, joint venture or other joint business relationship between the Parties or any of their affiliates, (ii) any fiduciary duty owed by one Party to another Party or any of its affiliates, or (iii) a relationship of employer and employee between the Parties.

l. *No Waiver*. Failure or delay on the part of either Party to exercise any right, power, privilege or remedy hereunder shall not constitute a waiver thereof. No provision of this BAA may be waived by either Party except by a writing signed by an authorized representative of the Party making the waiver.

m. *Severability*. The provisions of this BAA shall be severable, and if any provision of this BAA shall be held or declared to be illegal, invalid or unenforceable, the remainder of this BAA shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

n. *No Third Party Beneficiaries*. Nothing in this BAA shall be considered or construed as conferring any right or benefit on a person not party to this BAA or imposing any obligations on either Party hereto to persons not a party to this BAA.

o. *Headings*. The descriptive headings of the articles, sections, subsections, exhibits and schedules of this BAA are inserted for convenience only, do not constitute a part of this BAA and shall not affect in any way the meaning or interpretation of this BAA.

p. *Independent Contractors / No Agents*. Nothing contained in this BAA is intended to be, nor shall be deemed or construed to constitute Covered Entity and Business Associate as partners, joint ventures, co-principals, agents, or associates in connection with the Services and sharing of PHI, and Business Associate shall perform its duties and obligations hereunder as an independent contractor and not as an agent.

q. *Entire Agreement*. This BAA, together with any attached exhibits, statements of work, riders and amendments constitutes the entire agreement between the Parties hereto with respect to the subject matter hereof and supersedes all previous written or oral understandings, agreements, negotiations, commitments, and any other writing and communication by or between the Parties with respect to the subject matter hereof. In the event of any inconsistency between the provisions of this BAA and the provisions of the Service Agreement, the provisions of this BAA shall control as to the protection, use or disclosure of PHI. In the event of inconsistency between the provisions of this BAA and any mandatory provisions of the Privacy and Security Rules, as amended, or their interpretation by any court or regulatory agency with authority over Business Associate or Covered Entity, such interpretation or rule will control; provided,

however, that if any relevant provision of or amendment to the Privacy and Security Rules changes the obligations of Business Associate or Covered Entity that are embodied in the terms of this BAA, then the Parties agree to operate in compliance with the amendment, interpretation or provision and to negotiate in good faith appropriate non-financial terms or amendments to this BAA to give effect to such revised obligations. Where provisions of this BAA are different from those mandated in the Privacy and Security Rules but are nonetheless permitted by such rules as interpreted by courts or agencies, the provisions of this BAA will control.

r. *Regulatory References*. A citation in this BAA to the Code of Federal Regulations or the Privacy and Security Rules shall mean the cited section or rule as it may be amended from time to time.

s. *Reciprocal Obligations*. In the event that Covered Entity acts as a "business associate" to Business Associate, then Covered Entity shall provide the same protections as Business Associate hereunder to Business Associate and agrees to be bound by the terms of this BAA the same as Business Associate with respect to such PHI of Business Associate.

IN WITNESS WHEREOF, the Parties have executed this BAA contemporaneously with the effective dates of the Service Agreement.

(Business Associate)	**(Covered Entity)**
Signed	Signed
Printed	Printed
Date	Date

BUSINESS ASSOCIATE LISTING INFORMATION

In order to comply with the OCR request to provide detailed information about business associates, please provide the following information:

Type of Service(s) Provided: _____

Business Associate Privacy Officer
Name (printed): _____
Phone: _____
Address: _____
E-mail:_____

Business Associate Security Officer
Name (printed): _____
Phone: _____
Address: _____
E-mail:_____

Website URL: _____

Exhibit A

Indiana University Health, Inc. Security Requirements

These are minimum requirements required by IU Health's Information Security Program. We recognize that sound practices require continual assessment of evolving risks, technology and relevant issues related to information security. In the event that our Information Security Officer deems it necessary to modify these Security Requirements in order to continue to reasonably protect IU Health Confidential Information, then Business Associate will be notified and a remediation plan and timeframe will be mutually agreed upon. For the purposes of below, (i) each reference to "Agreement" shall be defined to include the BAA and Service Agreement, (ii) each reference to "Provider" shall be defined to include Business Associate, and (iii) each reference to "IU Health" shall be defined to include Covered Entity.

Any information technology system implemented as part of this Agreement that processes, stores, transmits, or receives information classified as Restricted or Critical by the IU Health Data Classification Policy is subject to the regulatory provisions regarding these data classifications, which include the Health Information Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI-DSS), Family Educational Rights and Privacy Act (FERPA), and the HITECH Act. Therefore, any such system implemented as part of this Agreement must:

i. Demonstrate that it stores data at rest in compliance with the HIPAA Security Rule or PCI-DSS as applicable by either utilizing existing Provider's facilities (e.g., storage area network, file servers) to store data, or utilizes NIST FIPS 140-2 compliant encryption to store it local to the system itself.

ii. Demonstrate that it is able to securely transmit and receive PHI in compliance with the HIPAA Security Rule, HITECH Act, or PCI-DSS by utilizing NIST FIPS 140-2 compliant encryption.

iii. Demonstrate that data access requires a unique username/password or two-factor authentication (e.g., username and password, along with a personal identification number, certificate, software or hardware token, or smart card).

    1. Ideally, the system will demonstrate that users can be provisioned from already-existing directory systems utilizing either LDAP/S or Identity Management technologies such as Active Directory, OpenAthens, Shibboleth, or login.gov through Active Directory Federation Services or integration technologies.

iv. Provide the ability to log and monitor access to data

    1. Log the date, time, user id, requesting Internet Protocol (IP) address, subject ID(s), and actions taken by users to query, read, add, modify, or delete data about said subject(s).

    2. Provide the ability to query the logging and monitoring data by user, date, workstation or subject, or export said data in a structured format for reporting purposes.

    3. Provide the ability to export the data so that IU Health can retain it in accordance with the Center for Medicare and Medicaid Services' Office of Civil Rights (OCR) guidance on Cloud Computing, PCI-DSS, and internal IU Health policies on data retention.

        a. Ideally, the system would allow IU Health to receive the data over syslog or a similar protocol allowing it to be transmitted to the hosted Security Incident and Event Manager (SIEM).

v. Allow installation of IU Health supplied digital certificates and certificate chains to facilitate encryption utilizing Transport Layer Security (TLS) version 1.2 or greater technologies.

   1. If the system does not support TLS 1.2 or greater, please document the resolution and steps to update the system to handle it with an estimated completion date.

vi. Allow backup and recovery of digital certificates and encryption technologies utilizing existing Provider systems.

vii. Demonstrate overall systems compliance by providing the following for mandatory review by IU Health's Information Security Team:

   1. An overall system architecture diagram, which includes a demonstration of logical separation of client data that prevents commingling of data.
   2. A recommended network architecture implementation, including recommended segmentation, firewall rules, and network protection such as Data Loss Prevention to allow only applicable ports & protocols to protect data.
      a. In the case of PCI-DSS compliance, this is required.
   3. A documented example of an actual system implementation.
   4. If this is a cloud-based or hosted system, a documented network architecture showing the security controls in place (e.g., firewalls, IDS/IPS, authentication, Data Loss Prevention, etc.).
   5. Provider references for security implementations.
   6. Demonstrated backup and recovery procedures.
   7. Demonstrated user access management procedures.
   8. Static code analysis utilizing a verified third-party tool to ensure provided source code does not have any security issues.
   9. A risk assessment of the application environment, with a documented issues list and plan to address discovered issues on at least an annual basis.
   10. A risk management plan to continually address and remediate discovered issues.
   11. Periodic vulnerability testing of the environment to discover and remediate potential vulnerabilities.
   12. If the system is handling PCI-DSS data:
      a. A third-party penetration test performed by a certified PCI QSA on a quarterly basis.
      b. If systems and data are to be hosted in a non-Provider location, please provide the following for any facility or third party which will be storing, hosting, or processing said systems or data:
         i. A Service Organization Controls 1 (SOC 1) Type 2 Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting.
         ii. A Service Organization Controls 2 (SOC 2) Type 2 Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

We require that both reports be completed to standards set by the American Institute of Certified Public Accountants (AICPA), and be completed by a licensed CPA firm.

13. A Data Destruction Policy which demonstrates that data no longer in use or required to be retained will be destroyed to National Association for Information Destruction (NAID – www.naidonline.org) standards.

viii. Provide support for the application(s) running on a defined set of:

1. Operating Systems and supporting system services (e.g., OpenSSH, OpenSSL, Apache, Systemd).
2. Relational Database Management System Software (e.g., Oracle, SQL Server, MySQL).
3. Third-party software such as Application Servers, Web Servers, Security Software, Support Libraries, and other software required for daily operation of the application(s)

ix. If there are discovered security vulnerabilities in the previously described items and/or the application(s), the following need to be provided within 48 hours to IU Health:

1. Mitigation steps that IU Health can undertake to mitigate the reported vulnerabilities.
2. A timeline for any application patches that need to be applied to the environment to mitigate vulnerabilities.
3. A timeline for testing and approval of patches to any of the supporting items described above.

x. If there are discovered security vulnerabilities in the previously described items and/or the application(s), the following need to be provided within seven (7) days to IU Health:

1. Instructions for patching the supported items to restore the security posture of the environment.
2. Instructions for patching the application to restore the security posture of the environment.

xi. Ensure that the Operating System, any Relational Database Management System Software, and Third-Party software is supported by both the system and/or software vendors for the system lifecycle with system updates and security patches. If any of these components become unsupported, the Provider needs to address this before the system has an unsupported component.

xii. Provide documentation on the organization's Incident Response Plan, and a current list of security contacts for reporting vulnerabilities or compliance issues.

xiii. Allow IU Health the right to audit information systems in the scope of the system(s) in scope of this Agreement.

xiv. Provide IU Health responses to the provided Vendor Risk Assessment and Security Questionnaire. Any misrepresentation on either of these documents may result in contract termination.

xv. Provide IU Health a data dictionary and instructions on how to extract data in a defined industry-standard format (e.g., Text, database backup, etc.) using industry standard methods that will allow retrieval and analysis to meet data retention guidelines as specified by federal and state law, and guidance issued by the Office of Civil Rights.

Lasalle University

Implementing Secure Cloud Computing in the Small to Medium-Sized Healthcare Environment

May 2012

LASALLE UNIVERSITY

Implementing Secure Cloud Computing in the Small to Medium-Sized Healthcare Environment

INL 880 Capstone Project

Mitch Parker and Javier Aguero

5/4/2012

Abstract: There is a growing push to have small to medium-sized healthcare providers adopt Electronic Health Record or Electronic Medical Records systems as part of Federal incentive programs. The costs of these systems are causing vendors to look at cloud-based systems to host their data. We look at the potential risks and devise system selection, mitigation, and implementation strategies to provide organizations with the ability to secure their data both locally and in the cloud.

Contents

Executive Summary 3
Introduction 4
EMR Technologies and the Current Situation with Meaningful Use Certification 8
Requirements Mapping and Development of a Security Evaluation Instrument 11
Developing Secure Solutions 13
- Encryption 18
- Technical Policy and Unique User Identification/Access Control 25
- Proxy Server and Data Loss Prevention 28
- Firewall 31
- Antivirus 32
- Policies, Procedures, Risk/Impact Analysis, and Contracts 32
- Proof of Concept Implementation 34

Recommended Implementation Strategy 35
Benefits 40
Lessons Learned, Suggestions, and Conclusion 42
References 46
Appendix A- Cloud-based/Remotely Hosted Security Evaluation Matrix 58
- A – Encryption 58
- B – Technical Policy and Unique User Identification/Access Control 60
- C – Proxy Server and Data Loss Prevention 62
- D – Firewall 63
- E – Antivirus 64
- F – Policies, Procedures, Risk/Impact Analysis, and Contracts 65

Appendix B - Glossary 74

Executive Summary

There is a growing trend to have small to medium-sized healthcare providers adopt certified Electronic Health Records (EHR) or Electronic Medical Records (EMR) systems as part of Federal Meaningful Use incentive programs to modernize the delivery of healthcare. The major barrier to adoption of these systems is the implementation cost. There are multiple providers of outsourced and cloud-based certified EMR or EHR systems who promise to provide security that meets the required standards, which are defined in the Health Information Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and the Meaningful Use financial incentive programs from the Center for Medicare and Medicaid Services. These solutions can provide healthcare practitioners with significant cost savings over hosting their own EMR system.

The addition of an EMR system to a medical practice adds significant risk and the potential for financial and reputational damage because an unauthorized data breach is equally great. The addition of any EMR system to any medical practice requires additional security and processes. The implementation of a cloud-based or outsourced solution does not immediately provide the security an organization needs to protect them. There are multiple other factors which affect the security of any medical office or EMR system that need to be addressed.

This provides a comprehensive solution set to address these issues and mitigate risks. This involves the development of a selection instrument based on federal regulations which can be used by small to medium-sized healthcare providers to determine if their choice of cloud-based EMR systems meets the requirements as

stipulated under HIPAA, HITECH, and Meaningful Use. To address residual risk in the offices identified during the creation of the instrument, a vendor selection process based on the criteria in the instrument is used to find solutions to those issues. A recommended implementation strategy for a small to medium-sized healthcare provider is then provided. The benefits and lessons learned are then discussed along with salient points for the overall conclusion.

Introduction

Over the past few years, there have been multiple advances in technology and networking that have put the reach of large-scale networked systems within the hands of everybody, especially healthcare providers. Since 1985, when the Veterans Administration installed the first comprehensive Electronic Health Record, VistA, in all of its clinics (WorldVista Inc., 2012), there has been a push to utilize electronic medical records systems to store patient data and make it easily accessible to both providers and patients.

There has also been another push from within the medical field itself to use technology to provide better patient care. Many medical professionals, not just doctors, have availed themselves of the latest technologies to support their practices. Some of these technologies include smartphones, tablet computers, interactive web applications, and electronic medical records systems. Some of these allow for full access to patient charts and medical records. One of the largest vendors of Electronic Medical Records, Epic, offers an application for this called Haiku which runs on the iPhone (Epic Systems, 2012).

Recently, there have been three major pieces of legislation that have caused small to medium-sized medical practices to want to adopt Electronic Medical Records (EMR) or Electronic Health Records (EHR) systems. The first piece is the Health Information Portability and Accountability Act, known as HIPAA, which enforces stringent privacy and security rules, as well as standardized code sets for reporting transactions (CMS, 2012). HIPAA is a very important piece of legislation because it provides for patient privacy, through access to medical records by the patient and their designated appointees, and legal enforcement of the patient's privacy through specific violations (CMS, 2012). HIPAA is the major driver behind many of the practices in healthcare organizations today, because it mandates standardized code sets and reports along with privacy and security standards which EMR or EHR systems must follow.

The second piece is the amendment to HIPAA that is part of the American Recovery and Reinvestment Act of 2009, known as ARRA or the Stimulus Act (recovery.gov, 2012). ARRA includes a provision known as the Title XIII - Health Information Technology for Economic and Clinical Health Act and also known as the HITECH Act (GPO, 2009). The HITECH Act provides for stiffer penalties for organizations that violated HIPAA, up to $1.5 million per violation (GPO, 2009). It also requires organizations to be more proactive about weaving security into their mainstream activities (Long, 2011). And it also provides financial incentives for many types of medical providers, from small medical offices to large academic hospitals, to adopt Electronic Health Record or Electronic Medical Record technologies (GPO, 2009). These funds are dispersed when the organization demonstrates that the electronic health record systems are used and meet certain criteria.

The criteria for government financial incentives related to EMR are defined as part of the Center for Medicare and Medicaid Services' (CMS) Meaningful Use Incentive Programs (CMS, 2012). This is the third piece of legislation campaigning for Electronic Health Records (EHR). These three criteria, which were originally defined as part of the HITECH Act, include using an EHR in a certified manner, such as e-prescribing; using a certified EHR for electronic exchange of health information to improve quality of health care; and using certified EHR technology to submit clinical quality and other measures (CMS, 2012). Stage 1 of the incentive programs began in 2011, and Stages 2 and 3 will (tentatively) be implemented in 2013 and 2015, respectively (CMS, 2012). These programs are designed to advance medical practices toward full adoption of EMR/EHR systems.

These requirements and financial incentives signify a multifaceted problem. There are a large amount of smaller medical practices and healthcare organizations that would not be able to implement Electronic Health Records without the use of federal incentive dollars because of the high cost of implementation (Kumar and Aldrich, 2010). HIPAA Compliance is expensive, and is also often times confusing. A small industry of Electronic Health Record providers has emerged over the past several years offering certified systems for smaller providers. These systems are hosted in the cloud or remotely at other sites. The reason why remote hosting is implemented is because many medical practices cannot afford to host their own systems, or hire their own IT staff to maintain them (Valdes, Kibbe, Tolleson, Kunik, Petersen, 2004).

Therefore, smaller organizations consider implementing a lower-cost model, such as an Application Service Provider or Cloud Computing solution for their Electronic

Medical Records system. The cost savings of a cloud computing model as opposed to in-house can be anywhere from 50% to 90% of the final system cost (Mell and Grance, 2009). Cooper University Hospital realized significant implementation cost savings by outsourcing their Epic implementation to ACS. Michael Sinno, former CIO of Cooper University Hospital indicated that he was able to save costs and implement Epic for $18 million as opposed to the implementation costs for an in-house solution. In addition, there are other costs to consider in terms of system maintenance.

Cloud Computing is one of the latest buzzwords in IT computing, with multiple first-tier providers such as Amazon, Rackspace, and Intuit offering Software as a Service (SaaS) to customers. They offer systems where the customer pays for everything as a service in one bill, as opposed to multiple services or applications (Armbrust, 2010).

Most importantly, information loss or misuse because of a data or security breach becomes the problem of the provider (Nahra, 2008). The reputation of the providers themselves is compromised (Long, 2011). Therefore, there is a need for additional security and security processes in a small to medium sized provider environment, because putting an Electronic Health Record or Electronic Medical Record system in place adds a degree of risk that was not there before, especially if the solution is outsourced to one of the providers.

Organizations using outsourced solutions need to answer specific questions. First are these solutions really compliant when looked at in the context of their implementation in a medical office setting? Second, is a "cloud" solution secured, and can the risks be identified and mitigated? Third, what security is needed for computers in the offices or with devices that access the system? The chief issue with an EMR or EHR cloud solution

issue is that the implementation of a certified EHR system is only one component of Meaningful Use. A cloud-based solution, which may help an organization receive incentive money from the US Government, may not have the security that an organization needs to adequately protect its data. This is because the use of a certified system does not guarantee that the systems which access it are also secure.

This paper provides a framework for small and medium-sized healthcare organizations to effectively implement a cloud-based Electronic Health Record solution that will protect their patients, their organizations, and their employees. It focuses on technology strategies needed and provides a model to effectively implement the managerial and technical controls.

EMR Technologies and the Current Situation with Meaningful Use Certification

Currently, the most prevalent technology used in the healthcare environment is the Electronic Health Record (EHR) or Electronic Medical Record (EMR). The definition from the Department of Health and Human Services (HHS) is:

> An EMR (electronic medical record) is a real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians in decision-making. The EMR can automate and streamline a clinician's workflow, ensuring that all clinical information is communicated. It can also prevent delays in response that result in gaps in care. The EMR can also support the collection of data for uses other than clinical care, such as billing, quality management,

outcome reporting, and public health disease surveillance and reporting (HHS, 2012).

EMR systems can contain multiple modules, including Emergency Medicine, Laboratory Medicine, Radiology, Operating Room, Ambulatory Care, and Acute Care (Epic Systems, 2012). They are used to organize all of the information on a patient in one place, and can facilitate access by outside agencies or the patients themselves (Epic Systems, 2012).

Currently, the United States government provides financial incentives for adoption of EMR systems by practices and hospitals. This program, Meaningful Use, has been in place since 2010 (Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, 2010). Meaningful Use, which was originally part of the HITECH Act (Section 4101c), provides incentive payments to providers who adopt EMR technology. It also provides for financial penalties for organizations who do not adopt this technology by 2015 (Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, 2010). The penalties will be lower payment rates for organizations that do not adopt EMR or EHR systems.

The Certification Commission for Health Information Technology (CCHIT) is authorized by the Department of Health and Human Services to offer certification services under the guidance of the Office of the National Coordinator – Authorized Testing and Certification Body (ONC-ATCB) of the Department of Health and Human Services (HHS) (CCHIT, 2012). Only organizations that implement EMR systems which are certified by CCHIT with ONC-ATCB certification are eligible to continue to apply for incentive payments (CCHIT, 2012) (Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, 2010).

There are three categories of certification by CCHIT. The first is ONC-ATCB, which is the most rigorous, and ensures that the EMR that the organization is implementing meets the certification criteria established by the Secretary of the Department of Health and Human Services (CCHIT, 2012). The second is CCHIT Certified, which includes a rigorous inspection of integrated EHR functionality, interoperability, and security according to criteria independently developed by the CCHIT's multi-stakeholder and expert work groups using CCHIT's published testing methods (CCHIT, 2012). This does not necessarily include the certification criteria from the Department of Health and Human Services. Finally, there is the EHR Alternative Certification for Healthcare Providers, or EACH (CCHIT, 2012). This allows organizations that have developed their own EMR/EHR system to certify their system with CCHIT with the ultimate goal of attaining ONC-ATCB certification so that they qualify for financial incentives (CCHIT, 2012).

There are multiple issues with the implementation of EMR systems by healthcare providers. The first is the cost, which is the biggest barrier (Zhivan and Diana, 2012). EMR systems can cost over $100 million to implement for a large healthcare system, such as the Epic implementation undergone by Geisinger Health System. This system costs 4.6% of their $2 billion annual revenue to maintain (Geisinger, 2012). EMR systems can also fail if the organization does not adopt it as an overall strategy with support from top leadership and support from all stakeholders. An example is the failed $34 million dollar EMR initiative at Cedars-Sinai Hospital (Kumar and Aldrich, 2010). Additionally, there is the perception that the implementation may make the hospital or provider more inefficient (Zhivan and Diana, 2012).

Requirements Mapping and Development of a Security Evaluation Instrument

To properly define the requirements for an EMR/EHR system in a format that may be used to provide small and medium-sized businesses, a tool can be used as part of the systems selection process. The requirements for these systems need to be distilled down to a matrix which will cover all of the requirements, and whether they are the responsibility of the vendor/cloud services provider, health care organization, or both. T

The matrix instrument (found in appendix A) will provide organizations who are seeking to implement cloud-based or hosted Electronic Medical Records solutions with a checklist of controls to follow before a successful implementation of a system is hosted remotely or in the cloud. Following these controls will help an organization meet the requirements of the HIPAA Security Rule, Breach Notification Rule, ONC-ATCB, HITECH regulations, Healthcare Information Technology Standards Panel (HITSP) controls, and American Institute of Certified Public Accountants (AICPA) Service Operational Controls reporting requirements. The regulations do not make certain issues, such as the proliferation of removable storage and its impact on the HIPAA Security Rule, obvious. The requirement for encryption of data at remote sites is needed so that only authorized users can access protected health information in accordance with ONC-ATCB certification criteria.

The matrix lists the requirements from the HIPAA Security Rule, and then maps the Breach Notification Rule and HITECH Regulations on top of them. The ONC-ATCB certification requirements are also mapped. The HITSP controls are put on top of these to provide further assertions that these controls met both federal laws and industry

standards. An AICPA control for Service Level Agreements was added so that organizations have the ability to have a contract in place that defines and measures service levels as the first requirement (AICPA, 2011). Finally, the Service Organization Controls SOC 2 reports requirements for remotely hosted data services were added. The purpose of SOC 2 reports is to measure the effectiveness of the relevant controls that an organization implements to protect the privacy and security of a system. If the hosting organization cannot meet SOC 2 requirements, it means that it does not have effective policies and procedures in place for protecting data as per the HIPAA Security Rule. The SAS 70 report will no longer work (AICPA, 2011).

The matrix is broken down into six major categories to address the issues. The first category is Encryption, which addresses the requirements for encryption of data at rest and in transit. The second category is Technical Policy and Unique User Identification/Access Control, which covers the technical implementation of a multi-user system that handles Protected Health Information (PHI). The third category is Proxy Server/Data Loss Prevention. This addresses potential breaches caused by improper data transmission. The fourth category is Firewall, which addresses the protection of the network from unauthorized access. Fifth is Antivirus, covering the protection of PCs and devices from malicious software. Sixth and final is Policies, Procedures, Risk/Impact Analysis, and Contracts, which cover the non-technical aspects of system implementation, specifically with organizational policies and procedures, system certification, business associate agreements, and risk/business impact analysis.

The matrix provides clarity throughout the system implementation process. While there are many sets of rules, this tool provides a comprehensive guide that can be

used as a checklist to protect their organization by making sure that the solution is the right choice for compliance with the rules in the first place.

Developing Secure Solutions

One of the major issues with examining the myriad of regulations is having a small or medium-sized business effectively implement them. While a cloud-based solution may be able to provide security on the services side, the overall risk mitigation for the organization is not totally addressed. Kurt Long, in his article "Proactive Defense", from the July 2011 issue of Hospital and Health Networks, indicates that organizations need to implement the following Information security and Privacy technologies to become compliant:

1. Employ a reputable, specialized third party to perform a gap analysis of information security and provide a report for the board.
2. Implement technologies and associated policies for encryption of all portable devices.
3. Initiate breach monitoring and protection for all systems that access protected health information.
4. Automate detection of privacy breaches related to identity and medical identity theft and unauthorized employee access to celebrities, friends, family and neighbors' records.
5. Automate privacy audit reporting across all applications that access protected health information.
6. Ensure electronic health record and other application vendors produce audit trails.
7. Create a chief information security officer position empowered with the appropriate authority and resources to identify and mitigate privacy breaches (Long, 2011).

The selection matrix developed in the previous section not only addresses these issues, it also addresses several gaps that Long did not address, specifically encryption of data at rest, authentication of unique users to the EMR system, secure configuration of

endpoints, and network security. The matrix will be used to develop the criteria to evaluate the secure solution set.

Many small to medium-sized businesses still use consumer-level technologies such as Linksys routers or consumer-level PCs from stores such as Best Buy to run their businesses. The biggest risks for any solution that implements e-commerce, Cloud, or ASP technologies are the endpoints and server systems (Marchany and Tront, 2002).

One of the major reasons the Cloud is so attractive is because anyone can buy a computer and run the software from anywhere that has an Internet connection (Hawthorn, 2009). Today, especially with the number of persistent threats on the Internet, this is very risky behavior (Hawthorn, 2009). The current technology needed for checking a machine's health every time it logs into a web site, Network Access Control (NAC), requires a significant amount of hardware and software engineering, and requires significant organizational coordination (Snyder, 2012). Many small to medium-sized businesses, and even some of the larger-sized ones, just don't have the resources to implement this. In addition, a solution that keeps a customer from accessing what they need for business may cause more issues than it solves, and it may be career-ending for the IT consultant who implements it (Snyder, 2012).

The technical and policy solution proposal set is something that an organization can implement for a lower cost using a combination of Free or Open Source and commercial software to implement the suggestions in Long's article. Valdes, Kibbe, Tolleson, Kunik, and Petersen, in their article "Barriers to Proliferation of Medical Records", directly cite the use of Free and Open Source software as a way to help increase the adoption of EMR systems with practices (Valdes, Kibbe, Tolleson, Kunik,

Petersen, 2004). The strategy is a best of breed environment with a combination of Free and Open Source software combined with commercial software that meets the customers' needs.

Many small and medium-sized businesses cannot afford the managed security services provided by companies such as Dell, Symantec, IBM, Verizon, or TrustWave. However, many of them already have local consultants that help with their systems. These consultants can implement these systems and recommendations, and the instructions are already available on the Internet. If there is skilled help needed, there are multiple consulting companies that are able to help with implementing these solutions.

The use of the recommendations for network security will provide small to medium-sized organizations with the ability to meet HIPAA, HITECH, and ONC-ATCB regulations by using a lower-cost solution to replicate the same results as much more expensive solutions that larger businesses implement, with an emphasis on compliance that is enough to meet requirements without compromising security.

To solve for these issues, the Cloud-based/Remotely Hosted Security Evaluation Matrix will develop a set of technical and policy requirements. The options for each requirement will be examined, including advantages, disadvantages, and costs. After this is done, a final solution set will be chosen and then summarized.

To satisfy the technical controls, a protection profile needs to be developed. The operating system for the client workstations is assumed to be Microsoft Windows. Three of the major EMR software packages, which are Siemens Soarian, Cerner Millenium, and Allscripts, require Windows clients (Siemens, 2012) (Cerner, 2012), (Allscripts, 2012). In addition, Microsoft Windows had 88.69% of the operating system share for the time

period of May 2011 to March 2012 based on the NetMarketShare statistics, which were based on the usage logs of 12,049 service providers (NetMarketShare, 2012). Therefore, it is statistically very likely that an organization will be running Microsoft Windows. Customers should run Windows 7 Professional, Enterprise, or Ultimate Edition, as they can be joined to an Active Directory realm to enforce security policies (Microsoft, 2012). It can be purchased as either a standalone OS, as an upgrade from Windows 7 Home Premium or Starter Edition, or with a new PC from a manufacturer such as Dell (Microsoft Store, 2012).

Table 1: Microsoft Windows 7 Client Features

	Microsoft Windows
Market Share for May 2011-March 2012 time period	88.69%
Support from major EMR systems	Siemens, Cerner, Allscripts
Recommended Version	Windows 7 Professional, Enterprise or Ultimate

For server software, customers should run Windows Server Small Business Server 2011 or Server 2008 R2 as a small office server. The Windows Server platform, as of Q3/Q4 2009, according to International Data Corporation, had 73.9% of the server operating system market (Foley, 2010). It also comes with Active Directory, which allows for the effective management of users, computers, printers, groups, applications, and other directory-enabled objects from one central location (Microsoft, 2012). Windows Small Business Server 2011 also comes with Microsoft Exchange Server 2010 for e-mail, and supports BitLocker for server disk encryption, Windows Software Update Services, and SharePoint Foundation 2010 for collaboration (Microsoft, 2011)

(Techotopia.com, 2012). It is reasonably priced, with Dell supporting configurations that cost as little as $1,197.00 (Dell.com, 2012). Additionally, technologies such as Microsoft SQL Server, which is required by several management platforms, can run on Windows Server (Microsoft, 2012).

Table 2: Features of Windows Server

	Windows Server
Market Share as of Q3/Q4 2009	73.9%
Centralized management of users, computers, groups, printers, and applications	Active Directory
Built-in Encryption support	BitLocker
Software Updates	Windows Software Update Services
Collaboration Support	SharePoint Foundation 2010
E-mail Support	Exchange Server 2010
System Cost	$1197.00

There are six different protection categories from the matrix under the protection profile required for a small to medium-sized provider to have the correct technical controls in place to satisfy the technical protection profile. The categories are summarized below:

Table 3: Protection Categories

Category	Description
Encryption	Protects data on USB and removable disks, PCs, and servers by using encryption to protect the contents
Technical Policy/Unique User Identification and Access Control	Configures PCs to meet a minimum set of security criteria by implementation and enforcement of configuration controls, and provides for the authentication and identification of users in a multi-user environment.
Proxy Server and Data Loss Prevention	Prevents unauthorized breaches by monitoring client endpoint activity, sending data for further analysis to a Data Loss Prevention Server, and preventing unauthorized data transfers.
Firewall	An appliance that mediates access to the network given a set of rules on what connections to allow or deny.
Antivirus	Protects PCs against known or potential malware and threats.
Policies and Procedures	Provide the management frameworks to ensure accurate implementation of the EMR system.

These are the categories from the matrix which need to be satisfied to ensure that a provider meets the technical and policy requirements under the HIPAA Security Rule, HITECH Act, Breach Notification Rule, and ONC-ATCB requirements.

Encryption

For encryption, there are two different types of encryption to consider which are USB/Removable Disk and data at rest. Section A of the matrix, Encryption, addresses the requirements for encryption for both types. Since there are different product requirements for both types, they are evaluated as separate categories.

For USB/Removable Disk encryption, four products were considered. Each of these products is widely used already to protect data. The first option was TrueCrypt, which is an Open Source disk encryption platform which works on fixed disks and removable media (TrueCrypt, 2012). Next was McAfee's Encrypted USB Platform, which uses a combination of McAfee USB Flash Drives and management software to

manage encrypted removable media (McAfee, 2012). Third was Symantec Endpoint Encryption Removable Storage Edition, which allows usage of any USB drives with its management software to effectively manage removable media (Symantec, 2012). Fourth and final was Microsoft BitLocker To Go, which is built into the Windows 7 Ultimate and Enterprise Editions (Microsoft, 2012).

TrueCrypt is the only disk encryption system that will work on every major platform, including Windows, Linux, and Mac OS X (TrueCrypt, 2012). It is also free (TrueCrypt, 2012). However, the USB drive encryption is manual, and it does not provide automatic key management. This makes compliance with control A100, Emergency Controls; very difficult in that it would require a process step to store recovery keys for each piece of media encrypted (TrueCrypt, 2012). This would be onerous in a smaller office. It is also not FIPS 140-2 compliant, which causes control A105 to fail (TrueCrypt, 2012). Finally, it also does not have robust audit logging or tracking of drive usage, which causes control A103 to fail (TrueCrypt, 2012).

McAfee's FIPS 140-2 compliant platform requires special McAfee USB drives, and will work on Windows XP, Vista, and Windows 7 (McAfee, 2012). A 4 GB McAfee USB drive is $89.99 from CDW.com, with a minimum of 10 required to purchase (CDW.com, 2012). In comparison, a 4GB Lexar flash drive from newegg.com is $5.99 (Newegg.com, 2012). For management, logging, and emergency controls, ePolicy Orchestrator 4.0 (which requires Active Directory) and the license manager are also required (McAfee, 2012). These also have recurring licensing costs (CDW.com, 2012). McAfee ePolicy Orchestrator also requires software that needs to be run on Windows Server (McAfee, 2012). McAfee ePolicy Orchestrator costs $18.99 per user, plus

$2.462.00 for SQL Server 2008 R2 (CDW.com, 2012). A major disadvantage is the $89.99 cost per USB drive that can only be used with the system. However, it does meet all of the required controls.

Symantec's solution has extensive support for all USB flash drives, external hard disks, and even CD/DVD drives (Symantec, 2012). It is also able to integrate with the Symantec DLP solution (Symantec, 2012). It provides automatic key management and recovery (Symantec, 2012). In addition, it is also FIPS 140-2 compliant and can create self-extracting encrypted file archives, which support different distribution models (Symantec, 2012). It also requires a management server and Active Directory in the client environment to comply with control A100, Emergency Controls (Symantec, 2012). This solution costs approximately $50 per user per year to implement (CDW.com, 2012). It also complies with all of the required controls.

Microsoft's solution requires Windows 7 Ultimate or Enterprise Edition (Microsoft, 2012). It provides automatic key management and recovery with Active Directory (Burchill, 2010). It is also FIPS 140-2 compliant (NIST.gov, 2012). It can be configured extensively through Active Directory (Burchill, 2010). It does not provide the logging or auditing of USB drive usage that the McAfee or Symantec solutions provide, which causes control A103, Device and Media Controls, to fail (Beaver, 2009). There are also additional upgrade costs for implementing Windows 7 Ultimate or Enterprise. The cost to upgrade is $129.95 for Professional, $139.95 for Home Premium, and $169.95 for Starter Edition (Microsoft Store, 2012).

Based upon the requirements, the only recommended solution that meets all four requirements at a reasonable cost is Symantec Endpoint Edition Removable Storage

Edition. This solution uses any USB drive, and even supports burning CD-ROM disks (Symantec, 2012). It also allows for robust audit logging, key recovery from a management console, and FIPS 140-2 compliant encryption. While McAfee does have a solution that also meets all of the requirements, they require the usage of their flash drives, which is costly. BitLocker does not provide the logging or auditing required to prove that flash drives are encrypted. TrueCrypt is not certified, does not provide logging or auditing requirements, and is very difficult to manage as recovery keys have to be generated for each piece of encrypted media (TrueCrypt, 2012).

Table 4: Removable Storage Encryption Comparison Matrix

	TrueCrypt	**McAfee Encrypted USB**	**Symantec Endpoint Encryption**	**Microsoft BitLocker To Go**
Cost	$0.00	$89.99 per drive + $18.99/user for ePolicy Orchestrator license + $2462.00 for SQL Server	$50 per year	$129.95-$169.95
FIPS 140-2 Compliance	No	Yes	Yes	Yes
Key Management/ Emergency Access	Manual	Automatic	Automatic	Automatic
Logging	No	Yes	Yes	Does not provide proof of encryption
Requires special USB media?	No	Yes	No	No
Encrypts CD-ROM disks?	No	No	Yes	No
Recommended Solution	No	No	Yes	No

For Encryption of Data at Rest, four options were examined. Each of these solutions is already used to protect data in client environments. The first solution for encryption of data at rest that was examined was Symantec's PGP Whole Disk Encryption. McAfee Endpoint Encryption is evaluated for at rest, TrueCrypt was examined, and Microsoft BitLocker.

Symantec's PGP Whole Disk Encryption solution allows the entire hard disk of a target system to be encrypted (Symantec, 2012). It supports Windows 2000 through Windows 7 on the desktop, and Windows Server 2003 to 2008 R2 on the server side (Symantec, 2012). It also supports Linux and Mac OS X (Symantec, 2012). It requires an additional server component, PGP Universal Server, to manage it and bring it into compliance with control A111b, and Emergency Access by supporting emergency access and key recovery (Symantec, 2012). It is also certified for compliance with FIPS 140-2 and Common Criteria, satisfying control A105 – Encryption (Symantec, 2012). It also has extensive compliance reporting options (Symantec, 2012). The cost, however, for one machine per year is $154.00 for Essential Support (Symantec, 2012).

McAfee's Endpoint Encryption solution also allows the encryption of entire hard disks (McAfee, 2012). It supports Windows XP through Windows 7 on the desktop, and Windows Server 2003 to 2008 on the server side (McAfee, 2012). It supports Mac OS X and requires ePolicy Orchestrator to provide the management, emergency access, and key management components (McAfee, 2012). ePolicy Orchestrator also provides reporting, auditing, and proof of protection in reporting (McAfee, 2012). It is FIPS 140-2 compliant (McAfee, 2012). The cost of the license for McAfee Endpoint Encryption is $85.99 per license with one year of support (CDW.com, 2012).

TrueCrypt also supports the encryption of entire hard disks using multiple methods, including passphrases and key files (TrueCrypt, 2012). It supports Windows 2000 through Windows 7 on the desktop, and Windows Server 2000 to 2008 R2 on the server side (TrueCrypt, 2012). It supports Linux and Mac OS X (TrueCrypt, 2012). However, it requires manual management of key files and recovery disks for each PC to support recovery of and access to encrypted data (TrueCrypt, 2012). This can be very daunting for a small medical office. It is not FIPS 140-2 compliant, which causes control A105 – Encryption to fail (TrueCrypt, 2012). Due to its decentralized nature, TrueCrypt does not provide centralized management and proof of encryption, which causes control A103 – integrity to fail (TrueCrypt, 2012).

Microsoft BitLocker supports the encryption of fixed disks using passphrases, Active Directory credentials, or smart cards (Microsoft, 2012). It supports Windows 7 Enterprise or Ultimate editions only on the desktop, and Windows Server 2008 and 2008 R2 on the server side, which can limit its effectiveness (Microsoft, 2012). It is also FIPS 140-2 compliant (NIST, 2012). It uses Active Directory to manage keys and provides for emergency access (Burchill, 2010). However, like BitLocker to Go, it does not have robust reporting capabilities and cannot provide the reports required to show compliance (Beaver, 2009). It is free if purchased with Windows 7 Enterprise or Ultimate Edition (Burchill, 2010). However, this requires organizations to purchase upgrades if they are running Windows 7 Professional, Home Premium, or Starter Edition.

There are two factors to consider when looking at a full-disk encryption solution. First, small businesses cannot be expected to run two different encryption packages since this can confuse users. A security researcher, Matt Bishop, states that configuration

errors are the possible cause of more than 90% of computer security failures (Whitten and Tygar, 2005). A consistent interface and design are critical to ensuring that encryption solutions work correctly for regular users that need to use them because of security constraints (Whitten and Tygar, 2005). Second, the package should support reporting on fixed disks and USB flash drives in one module. Both the McAfee and Symantec solutions support this, while the Microsoft and TrueCrypt solutions are lacking (McAfee, 2012) (Symantec, 2012). The McAfee solution requires special USB flash drives, while the Symantec solution supports fixed disks, USB flash drives, and CD-ROM disks (McAfee, 2012) (Symantec, 2012).

It is due to these reasons that the Symantec solution is recommended for both USB and full-disk encryption. It meets the controls, and provides a consistent interface and reporting for both while allowing the customer freedom of choice to use whatever removable media they wish (Symantec, 2012).

Table 5: Fixed Disk Encryption Comparison Matrix

	Symantec PGP Encryption	McAfee Endpoint Encryption	TrueCrypt	Microsoft BitLocker
Cost	$154.00/year	$85.99/year	$0.00	$129.95-$169.95 for an upgrade
FIPS 140-2 Compliance	Yes	Yes	No	Yes
OS Support	Windows 2000-Windows 7, Windows Server 2003-2008 R2Linux, Mac OS X	Windows XP-Windows 7, Windows Server 2003-2008 Mac OS X	Windows 2000-Windows 7, Linux, Mac OS X	Windows 7 Ultimate, Windows 7 Enterprise, Windows Server 2008 R2
Automatic Key Management	Yes	Yes	No	Yes
Logging/Reporting	Yes	Yes	No	Does not provide proof of encryption
Recommended Solution	Yes	No	No	No

Technical Policy and Unique User Identification/Access Control

For Technical Policy, which governs the ability to configure PCs to meet a minimum set of security criteria by implementation and enforcement of configuration controls, and Unique User Identification/Access Control, two options were researched. The requirements for these were covered in Section B of the matrix. Those systems were Microsoft Active Directory Domain Services and Linux/Samba 4.

Microsoft Active Directory Domain Services comes standard with Windows Server, and provides a repository for configuration information, authentication requests, and information about the objects stored in it (Microsoft, 2012). It is designed to manage

corporate identities, credentials, and system and application settings (Microsoft, 2012). It also allows users to manage users, computers, groups, printers, applications, and other objects from one centralized platform (Microsoft, 2012). One of the components of Active Directory Domain Services is Group Policy. It is used to manage configurations for groups of computers and users, including options for registry-based policy settings, security settings, software deployment, scripts, and preferences (Rock and Stephens, 2012).

Active Directory Domain Services and Group Policy satisfy controls B100, Workstation Logical/Physical Security and B101- Access Control in that when a machine is joined to Active Directory, there is centralized management of who can access that machine or not (Microsoft, 2012). Active Directory can also be configured to satisfy controls B103 – Audit Controls and B106 – Non-repudiation/Centralized Authentication because Microsoft Active Directory utilizes the Kerberos Protocol to provide a degree of non-repudiation through using the Kerberos protocol for client/server authentication communication, and through its use of event logs to document authentication attempts on the client and server sides (Kerberos Consortium, 2012) (Microsoft Support, 2006). Audit controls B102 – Unique User Identification and B104 – Person or Entity Authentication are supported through the creation of unique user accounts which can authenticate to Active Directory (Microsoft, 2012). Audit Control B105, Consistent Time is satisfied by the use of the Windows Time Service to provide time synchronization between PCs and an Active Directory server that synchronizes to an NTP time source (Microsoft, 2010). Control B107 – Document Updates is satisfied by the use

of the Windows event log to document system and patch changes on each PC, which can be scripted and managed from a server (Microsoft TechNet, 2009).

Samba 4 is a Linux-based implementation of Microsoft's Active Directory and SMB/CIFS file and print-sharing protocols (Samba.org, 2012) (Edge, 2011). It is currently in beta stage (Edge, 2011). However, Samba has historically been used to provide a Free Software replacement to Microsoft's proprietary authentication systems so that true interoperability can be achieved (Samba.org, 2012). Many corporations have utilized Samba to provide a Free Software alternative to Windows Domains or Active Directory (Samba.org, 2012). However, Samba 4 requires the use of an NTP daemon on each client to synchronize time (Corbet, 2012). It also uses the UNIX logging format to log events and errors, which is not consistent with Windows (Eckstein, Collier-Brown, Kelly, 1999). It can log to text files and also to syslog (Kukkukk, 2012). However, adding users to Samba requires using the Linux command line to run commands to do so (Red Hat, 2012).

Due to the fact that Samba 4 is currently in beta stage, and has significant issues that need to be resolved before a release date can be finalized, controls B100 – Workstation Logical/Physical Security and B106 – Non-repudiation/Centralized Authentication cannot be satisfied because the product still has major issues preventing the use of it in a production environment. Therefore, the use of Samba, which is historically the Free Software alternative to Microsoft Windows Server and Active Directory, cannot be recommended. Microsoft Active Directory, which meets all of the required security controls, and has also been a proven product in the marketplace, is the recommended solution.

Table 6: Technical Policy Comparison Matrix

	Microsoft Active Directory	**Samba 4**
User Authentication	Yes	Yes
In Production	Yes	Beta, no certain release date
Requires additional software?	No	Yes, NTP needed to synchronize time
Requires command line to add users?	No	Yes
Logging in same format?	Yes	No
Management of machines and objects via Group Policy?	Yes	Beta
Non-repudiation of authentication requests?	Kerberos	Beta
Cost	Requires Windows Server License	Free
Recommended Solution	Yes	No

Proxy Server and Data Loss Prevention

To evaluate Proxy Server and Data Loss Prevention solutions three proxy server and three data loss prevention software options are available. They work to mediate Internet access and can help guard against potential breaches by ensuring that data is not transmitted insecurely. The requirements for these are covered in Section C of the matrix.

Proxy servers need to support the Internet Content Adaption Protocol (ICAP), which allows a web proxy to pass messages to another server to be modified in transit (Elson and Cerpa, 2003). There are three widely-used proxy servers on the market which support ICAP. They are the Blue Coat ProxySG 300, WebSense, and Squid, which is the Open Source solution (Blue Coat, 2012) (WebSense, 2012) (Rousskov, 2012). The Blue Coat proxy solution costs $5,785.00 plus yearly support costs (Edgeblue.com, 2012).

The WebSense solution costs $13,440.00 plus yearly user licenses and support for the appliance (SecureHQ.com, 2012). The Squid solution is Open Source, is bundled with many Linux distributions and firewall appliances, and is free (squid-cache.org, 2012). Due to the fact that many small to medium-sized businesses will not be able to afford the Blue Coat or WebSense solutions, and the Squid solution supports the same required features, this is the preferred solution for the proxy server.

Table 7: Proxy Server Comparison Matrix

	Blue Coat ProxySG 300	**WebSense**	**Squid**
ICAP Support	Yes	Yes	Yes
Cost	$5,785.00 + yearly support	$13,440.00 + yearly support	$0.00
Recommended Solution	No	No	Yes

For the Data Loss Prevention servers, the solution needs to support scanning e-mail, web proxy servers via ICAP, and endpoints via a local agent. It also needs to support user-configurable rules. This will help satisfy controls C100 – Transmission Security, C101 – Protection against unauthorized disclosure, and C102 – Device and Media Controls, by giving organizations the ability to prevent unauthorized disclosure via the use of data loss prevention software, and the ability to track the transfer of ePHI onto electronic media that can be removed from the facility. Symantec, McAfee, and myDLP offer solutions which meet the requirements. Symantec offers Symantec DLP-9, which is a smaller version of their larger DLP product that can interface with web proxy servers and has an endpoint client that reports into a central server (Craig, 2009). McAfee offers McAfee DLP Endpoint and McAfee DLP Prevent, which can be combined with ePolicy Orchestrator to form a DLP solution that handles web proxies and endpoints (McAfee,

2012). MyDLP offers a Linux-based virtual machine appliance that interfaces with ICAP-compliant web proxy servers, e-mail, has an endpoint client that reports back to the virtual machine, and is also Open Source (mydlp.com, 2012). The Symantec solution starts at a base price of $25,000 plus yearly support (Craig, 2009). The McAfee solution requires ePolicy Orchestrator, costs $29,800.00 for the software, $35,000 for the DLP appliance, and additional yearly costs for the ePolicy Orchestrator license and yearly support (Stephenson, 2007). All of these products support user-configurable rules (Craig, 2009) (Stephenson, 2007) (mydlp.com, 2012).

The myDLP solution offers the same basic features as the Symantec and McAfee solutions, but has the benefit of being Open Source and free for download. It provides the same features as the much more expensive Symantec and McAfee solutions at a much lower cost, and can use older hardware or a virtual machine to host it. MyDLP is the recommended solution due to its cost and support for all requirements.

Table 8: DLP Software Comparison Matrix

	Symantec DLP-9	**McAfee DLP Prevent**	**myDLP**
Cost	$25,000 + support	$29,800 for software, $35,000 for DLP appliance, and additional license costs	$0.00
Web Proxy Support	Yes	Yes	Yes
Endpoint Support	Yes	Yes	Yes
E-mail Support	Yes	Yes	Yes
Virtual Machine Support	Yes	No	Yes
Recommended Solution	No	No	Yes

Firewall

The requirements for a firewall solution were developed in Section D of the matrix. For selecting a firewall solution, there were three Open Source packages considered: PfSense, m0n0wall, and IPCop. These are all packages that are designed to take older PCs which are not capable of running Windows 7 and turning them into robust firewalls. A decent firewall should have robust logging, an Intrusion Detection System (IDS), and the ability to be configured to protect against unauthorized intrusions.

PFSense comes with the ability to integrate an Intrusion Detection System, Intrusion Prevention System, robust logging, and Squid Proxy with ICAP support into the base firewall system (squid-cache.org, 2012)(pfsense.org, 2012). IPCop has a decent firewall built in and the ability to log to multiple sources, but does not have IDS (Ipcop.org, 2012). M0n0wall has a firewall and robust logging, but does not have an integrated proxy or IDS (Buechler, 2008). Out of the three solutions, PFSense meets the stated requirements, which were D100 – Protection against unauthorized disclosure, D101 – Physical Safeguards, and D102- Integrity. It is the recommended solution.

Table 9: Firewall Appliance Comparison Matrix

	PFSense	**IPCop**	**M0n0wall**
Firewall	Yes	Yes	Yes
IDS	Yes	No	No
IPS	Yes	No	No
Logging	Yes	Yes	Yes
Squid Proxy with ICAP Support	Yes	No	No
Cost	$0.00	$0.00	$0.00
Recommended Solution	Yes	No	No

Antivirus

To select an Antivirus solution that would meet the requirements developed in Section E - Antivirus, the criteria used was a solution certified by an independent testing laboratory, ICSA Labs (ICSA Labs, 2012). ISCA Labs, a division of Verizon Business, publishes a list of certified Anti-Virus products (ICSA Labs, 2012). The only corporate anti-virus solution on their list of products was the AVG Anti-Virus Business Edition (ICSA Labs, 2012). Solutions from Symantec, McAfee, Trend Micro, and Kaspersky were all certified for home usage, but not for corporate use by ISCA Labs. This costs $89.99 for two machines per year, which averages out to $45 per machine (AVG.com, 2012). While there are other products out there that are supported in corporate environments, they have not undergone scrutiny by an independent testing laboratory. A certified solution means that the product will be able to adequately protect the environment against threats. The controls satisfied by an antivirus solution were E100 – Integrity, and E101 – Protection against unauthorized disclosure. The recommended solution is the AVG Anti-Virus Business Edition product.

Policies, Procedures, Risk/Impact Analysis, and Contracts

The most comprehensive set of requirements is in Section F – Policies, Procedures, Risk/Impact Analysis, and Contracts. This section of the matrix covers the required policies and procedures for securely implementing an EMR system within a medical facility. There are a significant amount of controls required to satisfy requirements here.

To satisfy them, a multi-faceted approach is recommended. First, the organization needs to engage the services of a consulting group focused on small to

medium-sized businesses that can provide policy templates and advice, as well as risk assessment services (Long, 2011). It is recommended that the organization also customize the templates to meet the requirements of the organization and the issues discovered during the risk assessment. One of the organizations that performs these services, the Supremus Group, offers packages for organizations to not only provide policy templates, but also provides certification training for employees (Supremus, 2012).

Secondly, the organization needs to engage the services of a lawyer to review their contracts to ensure that the contracts that they have meet Business Associate Agreement rules, and that they can correct any compliance issues (Tovino and Reisz, 2012). Additionally, the organization must ensure that their policies meet requirements. Next, they need to train and empower a staff member to look over logs and check for and help resolve compliance issues. This would be the equivalent of a CISO for a smaller business (Long, 2011). The computer systems in place will generate log files and warnings, and it is a requirement to monitor those. It is also a requirement to document changes, and not documenting them is a compliance issue. Therefore, it is important, even if the person is part-time on the task, to have someone dedicated to compliance, and empower him or her to ensure that the organization does what is required. The HIPAA Security Rule mandates this review process, and Long's article further underscores that need.

Finally, a lawyer or other qualified professional with an understanding of the HIPAA Security Rule should review the proposed solution to ensure that it really does meet the stated requirements. It is key to understand how the operations of a remotely

hosted system operate and prove the solution is compliant by matching known criteria and their contracts.

Proof of Concept Implementation

As part of this project, a small proof of concept solution was developed using the pfSense firewall and myDLP Data Loss Prevention software. This was put together to prove that the recommended software would work in a small office environment. A Dell Dimension 3000 with 512 megabytes of RAM, an eighty gigabyte hard drive, and two network cards were used to house the pfSense firewall. A Dell Dimension 3000 with 768 megabytes of RAM and an eighty gigabyte hard drive were used to house the myDLP Data Loss Prevention server. The myDLP server was connected to the firewall on a switched network. The firewall was connected to a Comcast cable connection.

The pfSense solution is packaged as a CD image. This was downloaded from their web site and burned to a CD. The Dell Dimension was then booted to the CD. Installation of the software to the hard drive took approximately ten minutes. Configuration of the software, including specifying IP addresses and basic firewall rules, took approximately thirty minutes. Updating the software to the latest version and installing the Snort IDS/IPS and Squid proxy caching software took another thirty minutes. Configuring Squid for ICAP proxy access took another five minutes. The result was a firewall appliance that had a full IDS and IPS, along with an ICAP-compliant proxy server.

The myDLP solution is also packaged as a CD image based on Ubuntu Linux. This was also downloaded from their web site and burned to a CD. The other Dell Dimension was booted from it, and the software was installed from it. It took

approximately thirty minutes to install the software and assign an IP address to the server. It took thirty minutes to configure myDLP using an online tutorial and its web-based interface to accept traffic from the pfSense server, have a basic rule set in place to monitor for Social Security Numbers and credit card numbers, and block their transfer via the web or to a USB flash drive. Installation of the client on a Windows 7 PC on the same network required the use of a Microsoft Installer package and development of a small script to point the workstation to the myDLP server.

The result here was an endpoint solution which is capable of examining data transfer from a workstation, and is able to block and log potential breaches. The solution was implemented using lower-cost hardware which is not capable of running Windows 7. The software was capable of detecting social security numbers and credit card numbers, and was able to block their unencrypted transfer over the Internet and to a USB flash drive plugged into a PC running the myDLP client.

Recommended Implementation Strategy

The implementation of any EHR or EMR system is a complex task. The road toward successful implementations has been marked by failures large and small. Cloud Computing adds on another level of complexity and security to the process. The recommendation for small to medium-sized medical practices that would like to reap the economic benefits of cloud-based EMR or EHR systems is to start by utilizing the HIPAA/HITECH/Breach Notification Rule/ONC-ATCB matrix to guide their compliance efforts internally. The purposes of this tool are to understand the real risks, and to mitigate them before attempting to shift the risk to someone else's system. While an Electronic Medical Records system in the cloud may be fully in compliance with

ONC-ATCB regulations, but the usage of a virus-infected PC on a Linksys router, or an insecure wireless access point at Starbucks is not. There is no magical "cloud dust" to make the organization secure and "get your money!", as much as some of the ads out there would like to tell you otherwise (Longwood Systems, 2012).

The recommended implementation strategy consists of several parts. The goal here is to list the steps so that a small to medium-sized organization can easily implement and spread the costs across a period of time, and develop a security process, not just a point solution to implement Cloud. The implementation of an Electronic Medical Records system can be very costly and time-consuming. The goal is to provide understanding of the processes and a gradual implementation of a new cloud-based system so that it meets rules and regulations. The end goals, however, are security and protection of patient data.

The first step is to train the workforce. HIPAA and HITECH training from a reputable training company will provide the workforce with the understanding of what to do, what the penalties are, and most importantly, sets expectations as to how to perform (Long, 2011). The article "Hand Hygiene Compliance Among Health Care Staff and Student Nurses in a Mental Health Setting", by Marilyn Ott, RN, BScN, MScN, and Rachel French, RN, discusses a similar compliance issue which healthcare providers are dealing with, which is hand washing compliance for infection control. Ott and French discuss an approach where positive behavior modeling is used with continual training and cultural reinforcement, along with visual aids to provide an effective approach to compliance improvement in the healthcare environment (Ott, 2009).

Providing training as opposed to creating a culture of fear will reduce errors and provide understanding of the HIPAA Privacy and Security rules. The article "Brief Reports: The Impact of Fear of HIPAA Violation on Patient Care", by Bryan K. Touchet, M.D., Stephanie R. Drummond, D.O., and William R. Yates, M.D, touches on the fact that easily preventable errors have occurred because of fear of violating HIPAA, failure to understand the HIPAA Privacy Rule, and ethical concerns about HIPAA (Touchet, 2004). Training costs can range from $25.00 per person for online training costs from Evolve Healthcare Training, to $2,700 per person for in-person training from the Supremus Group (Evolve Healthcare Training, 2012) (Supremus, 2012).

The recommendation is to train the workforce using a reputable consulting firm that understands the HIPAA Privacy and Security rules, and the HITECH Act. The goal is to build a culture of positive reinforcement. The more understanding there is of what to do, the less fear will exist. Positive reinforcement is much more effective than punitive reinforcement (Ott, 2009).

Secondly, it is recommended that the organization contact an attorney or legal counsel that can help them review their contracts, business associate agreements, policies, and procedures to ensure they are in compliance with the HIPAA Security Rule and HITECH, as there are major changes which can affect the organization (Tovino and Reisz, 2012). The organizational policies of the business should be updated to reflect required changes with HIPAA and HITECH, and that the changes are socialized with the entire workforce (Long, 2011). The Digital Business Law Group charges between

$5,000 and $7,500 for a HIPAA audit that includes recommended changes to these agreements, policies, and procedures (Digital Business Law Group P.A., 2012).

Next, the security recommendations should be implemented internally in the office on the computers. The goal is to ensure that the computers which will be accessing the cloud computing solution are protected from malware via an antivirus implementation, have current security patches, are encrypted, have protection against unencrypted data being lost via USB drives or stolen/lost PCs, and that each user has a unique username and password to authenticate to resources internally. A powerful network firewall solution should be implemented. Data Loss Prevention software is also recommended to track PHI as it enters and leaves the office environment, and to block any potential breaches. The goal will get the organization to a point where the computers themselves will have a significantly higher degree of protection, will be in compliance with HIPAA, HITECH, Breach Notification Rule, and ONC-ATCB regulations, and will get them ready to use remotely hosted services.

Furthermore, organizations should have a comprehensive plan for standardizing and upgrading their hardware from three to five years so that they can run current software and enjoy the benefits of the latest protection methods (Ray, 2009). The instrument should be used as a continual compliance checklist for the organization going forward in combination with training. It is important that the organization be aware of the rules, and has a quick reminder of how to stay in compliance. The organization should hire a consultant to conduct a risk assessment and a Business Impact Analysis (BIA), as this is required by the HIPAA Security Rule and Meaningful Use regulations (Long, 2011). A plan should address the outstanding risks in the risk assessment.

(Medicare and Medicaid Programs, 2010). Using the Business Impact Analysis calculator from continuitycompliance.org, a BIA for a business with 10-49 employees, $2.5 million in revenue, and twenty critical business processes will require 76.75 hours of work for a full BIA (ContinuityCompliance.org, 2012). A consultant, at a rate of $100 per hour, will cost $7675 to perform this engagement.

Fourth, the organization should utilize the compliance instrument developed as part of an initial vendor selection process for a cloud-based EMR/EHR system. The small to medium-sized providers should do their own search for ONC-ATCB certified providers who meet their business needs, starting with the CCHIT website, and proceed to use the instrument to determine who meets HIPAA Security Rule, HITECH, Breach Notification Rule, and ONC-ATCB certification requirements.

Fifth, the organization should utilize the set of providers that comes from the initial selection process to find a vendor that meets their requirements and provides a supportive workflow (Miller and Sim, 2004). This will help make a decision that is based upon more than a presentation. The organization should also retain an attorney to go over the vendor contracts and make sure that everything meets Business Associate Agreement requirements. This can cost $100 to $500 an hour, depending upon the complexity of the contract and the skill of the lawyers (Costhelper.com, 2012).

Sixth, the organization should make a decision and implement an EMR system based on the selection process. Using both the compliance instrument and their selection workflow, they should find a system that meets their workflow and security requirements.

Seventh, organizations should develop and maintain a list of metrics to monitor continually such as system uptime, help desk response time, application performance,

number of breaches, and report performance (Eckerson, 2011). Organizations should review these metrics monthly to gauge performance of the system, and the level of customer support they are receiving (Eckerson, 2011).

Eighth, organizations should be continually vigilant about their risk. Being a smaller provider does not exempt anyone from risk assessments (HIPAA Administrative Simplification, 2006). The organization should use a consulting firm or legal counsel to assist in performing regular risk assessments to demonstrate compliance with the HIPAA Security Rule. A staff member should be empowered to review systems access on both the cloud-based system and locally to continually evaluate compliance (HIPAA Administrative Simplification, 2006). Kirk Nahra, in his article "HIPAA Security Enforcement is here", recommends that companies pay close attention to public security breach reports, and continually assess policies and procedures to ensure compliance (Nahra, 2008).

The end product from this eight-step implementation recommendation strategy is that a smaller organization can use cost-effective means to effectively implement the security controls required by the HIPAA Security Rule, HITECH, Breach Notification Act, and ONC-ATCB certification for a cloud-based EMR. This will effectively save the organizations running their own in-house EMR system and will put security controls in place that will make the organization as a whole more secure. This prevents organizations from the potential risks caused by having false hope that an EMR implementation will solve all of their issues.

Benefits

There are several benefits of implementing the cloud-based Electronic Medical Records system utilizing the process and strategy developed. There is also one drawback, which is the potential overall cost. The benefits, however, are far-reaching.

The first benefit is a framework for organizations to be compliant, according to federal law. The strategy does not focus on a sudden implementation, but a framework for getting compliant using positive reinforcement, methodical steps, and mitigating risk at all levels.

The second benefit is that organizations will be able to provide evidence of compliance to the required federal agencies to receive Meaningful Use financial incentives for the implementation of a cloud-based EMR/EHR system. The augmentation and design of a network using lower-cost tools using our reference design, combined with the use of the instrument developed, should provide organizations with the information they need to not only be compliant on the EMR side, but in their office as well.

In addition to Meaningful Use financial benefits, there are also operational benefits to the organization as well. The article ”A Cost-benefit Analysis of Electronic Medical Records in Primary Care”, from The American Journal of Medicine, cites an estimated net benefit of $86,400 for a provider for a five year period when an organization implements Electronic Medical Records (Wang et al, 2003).

Miller and Sim, in their article “Physicians’ Use of Electronic Medical Records: Barriers and Solutions”, also cite the operational benefits of implementing EMR. They specifically cite that it allows physician practices to pursue more powerful quality-improvement programs than possible with paper-based records (Miller and Sim, 2004).

However, they indicate that the quality improvements depend heavily on the use of the EMR to accomplish key tasks (Miller and Sim, 2004).

The next benefit is that the implementation of this framework will provide organizations with insight into what data they have, how it is transferred, and where the risk lies with potential breaches. The implementation of a Data Loss Prevention system will provide organizations with an understanding of where their data goes. The organization will be more secure than before since they will be able to track their data and avoid potential breaches. Furthermore, this implementation of the required controls provides the organization with accurate logging track information of what data they own and what is being transferred.

The final benefit is that following the strategy will increase the overall security of the organization. Where an EMR is hosted is only part of the picture. The other part is what machines access it, and how they are secured. Even if there is encryption and security on a cloud-based system, the biggest weakness is still the endpoint. Increasing the security of the endpoints and how they are managed helps mitigate larger risks to the organization.

While there is a cost to implementing any Electronic Health Record or Electronic Medical Record system, there is also conversely the threat of being paid less by Medicare for not implementing such a system (Medicare and Medicaid Programs, 2010). Usage of a cloud-based system costs significantly less than trying to implement a product in-house. The goal of what was done here is to implement such a system and meet security controls.

Lessons Learned, Suggestions, and Conclusion

The most important lesson learned is that security around cloud-based systems involves a lot more than just the cloud-based system. Everything which needs to access the EMR needs to be as secure as it, as well as the policies and procedures governing its use. There are multiple security criteria surrounding any machine that contains Protected Health Information, not just the EMR. The biggest potential security hole may be the workstations themselves, and there is not clarity between the HIPAA Security Rule, HITECH Act, and the Breach Notification Rule with regards to encryption. The ONC-ATCB regulations for certified EMR/EHR systems provided the required clarity with regards to encryption and security, however.

Any organization that wants to connect to the cloud for their business requirements needs to get their house in order first by implementing required policies and procedures, and putting a network in place that is capable of handling the security requirements on multiple levels (Long, 2011). A lost USB flash drive that may contain patient information could have devastating financial and reputational consequences for small to medium-sized organizations (Nahra, 2008).

The group of cloud-based providers should be more realistic with their customers. Many advertisements indicated how much money an organization could make by implementing an electronic medical records system, as opposed to how the solution could provide benefit to the organization as part of an overall security package. Providers should be realistic as to the amount of training required to implement an EMR. The Department of Health and Human Services should be clear on customer expectations.

Many systems which advertise themselves to be HIPAA compliant are not. In particular, the GE Radiology Information System that was implemented at Temple

University Hospital used unique user names and passwords for the end users, but not for the GE technical support staff or the system services. Internal Auditors flagged this as part of a routine post-implementation audit. This means that this particular vendor will need to redesign a multi-million dollar system and their internal support processes to be in compliance with the HIPAA Security Rule.

Another example is a Meaningful Use risk assessment for a community hospital located in Philadelphia. This hospital, to save costs, utilized an Application Service Provider for their EMR system. A CPA firm was engaged to provide a privacy and security assessment of the third-party vendor. As part of this engagement, two findings were discovered. The first was that the vendor had not filed a SAS 70 or SOC 2 privacy and security controls report for several years. Secondly, upon further research, it was discovered that the company was granting unauthorized users access to the databases that contained protected health information of its customers with no need to know.

Staff needs to be made aware that even though a software package may be HIPAA-compliant, the installation and configuration of the package may not be if the system itself is configured with generic accounts. As part of the audit of the Medhost Emergency Department Information System at Temple University Health System, the sole finding found was a procedural issue where generic usernames were given out to staff to view data in an otherwise completely compliant system. Internal Audits went to several departments to find out that user rights were improperly assigned. Several departments had to change how user access was provisioned based upon this finding.

Implementing a Data Loss Prevention system takes more work than just dropping something on the network and being punitive toward end users. Much of the

implementation time requires speaking with the stakeholders and training the end users. There has to be education including a training program, and there needs to be time spent hand-holding with the users. Security controls cannot simply be implemented and expected to work without training and sitting in the line of fire with customers.

It is entirely possible for a small to medium-sized healthcare organization to implement a cloud-based EMR that meets HIPAA, HITECH, Breach Notification Rule, and ONC-ATCB guidelines; it is a solution that can save organizations money as opposed to running an EMR in-house. However, the issue is that the organizations need to lock down and secure the PCs that will access the EMR first, get their own policies, procedures, and contracts in order, and continually monitor their own systems for uptime, and themselves for compliance.

Small to medium-sized providers will need to use a robust systems selection process to vet cloud-based systems based on their conformance to the required federal guidelines. They need a strategy based upon a systemic implementation of training, contract analysis, risk assessment, technology implementation in the office, vendor selection, and monitoring.

Technology in healthcare is a reachable goal, even with all the regulations out there. There is a lot of confusion and misunderstanding as to what to do. There are many Cloud vendors who are not secure. The goal is to help organizations avoid them, implement secure solutions, and continually stay compliant.

References

AllScripts Corporation (Allscripts) (2012). System Environment Specifications Network PC, Peripheral& Server Requirements. Retrieved on April 8, 2012 from http://www.allscripts.com/content/dam/allscripts/documents/MyWay_8.6_SystemEnvironmentSpecs.pdf

American Institute of Certified Public Accountants (AICPA) (2011, May 1). Service Organizations. Applying SSAE No. 16, Reporting on Controls at a Service Organization (SOC 1), New York, NY: AICPA.

Armbrust, Michael et al. (2010). A View of Cloud Computing. Communications of the ACM, April 2010, Volume 53, No. 4, pp. 50-58.

AVG.com (2012). AVG Anti-Virus Business Edition 2012. Retrieved on April 12, 2012 from http://www.avg.com/us-en/antivirus-business

Beaver, Kevin (2009). Considerations for BitLocker in Microsoft Windows 7. Retrieved on April 8, 2012 from http://www.principlelogic.com/docs/BitLocker_in_Windows7.pdf

Beck, Micah, Moore, Terry, Plank, Jim, Swany, Martin (2012). Logistical Networking: Sharing More Than the Wires. Retrieved on March 16, 2012 from http://loci.cs.utk.edu/ibp/files/pdf/LogisticalNetworking.pdf

Biswas, Kamanashis, and Islam, Md. Ashraful (2009). Hardware Virtualization Support in Intel, AMD, and IBM POWER Processors. (IJCSIS) International Journal of Computer Science and Information Security, Vol 4, No. 1 & 2, Retrieved on March 10, 2012 from http://arxiv.org/pdf/0909.0099.pdf

Blue Coat (2012). Blue Coat Full Proxy Edition –ProxySG 300/600. Retrieved on April 9, 2012 from http://www.edgeblue.com/datasheets/Blue_Coat_ProxySG_300-600_Full_Proxy.2.pdf

Blue Coat (2012). ICAP Data Trickling. Retrieved on April 9, 2012 from http://www.bluecoat.com/sites/default/files/product_tech_primers/ICAP_Data_Trickling.7.pdf

Breach Notification for Unsecured Protected Health Information (2009), 74 Fed. Reg. 42740 (to be codified in 45 CFR parts 160 and 164).

Buechler, Chris (2008). M0n0wall Handbook. Retrieved on April 10, 2012 from http://doc.m0n0.ch/handbook/

Burchill, Alan (2010, September 1). Best Practice: How to use Group Policy to save "BitLocker to Go" recovery keys in Active Directory – Part 1. Retrieved on March 15, 2012 from http://www.grouppolicy.biz/2010/01/how-to-use-group-policy-to-save-bitlocker-to-go-recovery-keys-in-active-directory-part-1/

CDW.com (2012). McAfee Endpoint Encryption for PCs – license. Retrieved on April 8, 2012 from http://www.cdw.com/shop/products/McAfee-Endpoint-Encryption-for-PCs-license/1439970.aspx

CDW.com (2012). Search Results for McAfee USB Drives. Retrieved on April 8, 2012 from http://www.cdw.com/shop/search/result.aspx?key=mcafee+usb+drives&wclsscat=&b=&p=&searchscope=All&ctlgfilter=&sr=1

CDW.com (2012). Symantec Endpoint Encryption Removable Storage Edition (v. 8.2) – license. Retrieved on April 8, 2012 from http://www.cdw.com/shop/products/Symantec-Endpoint-Encryption-Removable-Storage-Edition-v.-8.2-licen/2495745.aspx

Center for Medicare and Medicaid Services (CMS) (2012). CMS EHR Meaningful Use Overview EHR Incentive Programs. Retrieved on March 5, 2012 from https://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp

Center for Medicare and Medicaid Services (CMS) (2012). HealthIT.hhs.gov: Electronic Medical Records. Retrieved on March 1, 2012 from http://healthit.hhs.gov/portal/server.pt/community/electronic_medical_records/1219/home/15591

Certification Commission for Health Information Technology (CCHIT) (2012). About the Certification Commission for Health Information Technology. Retrieved on March 1, 2012 from http://www.cchit.org/about

Certification Commission for Health Information Technology (CCHIT) (2012). What is the ONC-ATCB 2011/2012 Certification Program? Retrieved on March 1, 2012 from http://source.cchit.org/web/source/source-more

Certification Commission for Health Information Technology (CCHIT) (2012). CCHIT Certified 2011. Retrieved on March 1, 2012 from http://www.cchit.org/get_certified/cchit-certified-2011

Certification Commission for Health Information Technology (CCHIT) (2012). What is EACH?. Retrieved on March 1, 2012 from http://each.cchit.org.

Center for Medicare and Medicaid Services (CMS) (2012). HIPAA Administrative Simplification Statute and Rules. Retrieved on March 3, 2012 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

Cerner Corporation (Cerner) (2012). Cerner and HP. Retrieved on April 8, 2012 from http://cerner.com/About_Cerner/Partnerships/HP/?LangType=1033

Chen, Yanpei, Paxson, Vern, and Katz, Randy H. (2010, January 20). What's New About Cloud Computing Security? Retrieved on March 7, 2012 from http://www.utdallas.edu/~mxk055100/courses/cloud11f_files/what-is-new-in-cloud-security.pdf

City of Philadelphia (phila.gov) (2012). Phila.gov | Public Health, Division of Disease Control, Epidemiology Program. Retrieved on February 5, 2012 from http://www.phila.gov/health/DiseaseControl/Epidemiology.html

Congdon, Kenneth (2009). How Much Will an EHR System Cost You? Healthcare Technology Online. Retrieved on March 1, 2012 from http://www.healthcaretechnologyonline.com/article.mvc/How-Much-Will-An-EHR-System-Cost-You-0001

ContinuityCompliance.org (2012). Business Impact Analysis Calculator. Retrieved on April 12, 2012 from http://www.continuitycompliance.org/tools-resources/community-projects/business-impact-analysis/

Corbet, Jonathan (2012, January 16). LCA: A Samba 4 Update. Retrieved on April 8, 2012 from http://lwn.net/Articles/475592/

Costhelper.com (2012). How much does a licensing contract cost? Retrieved on April 12, 2012 from http://smallbusiness.costhelper.com/licensing-contract.html

Cox, S, Wilcock, P and Young, J (1999). Improving the repeat prescribing process in a busy general practice. A study using continuous quality improvement methodology. *Qual Health Care* 1999;**8**:119-125 doi:10.1136/qshc.8.2.119

Cristiano, J. J., Liker, J. K. and White, C. C. (2000), Customer-Driven Product Development Through Quality Function Deployment in the U.S. and Japan. Journal of Product Innovation Management, 17: 286–308. doi: 10.1111/1540-5885.1740286

Department of Homeland Security (DHS) (2012). Business Impact Analysis | Ready.gov. Retrieved on March 12, 2012 from http://www.ready.gov/business-impact-analysis

Department of Homeland Security (DHS) (2012). Risk Assessment | Ready.gov. Retrieved on March 12, 2012 from http://www.ready.gov/risk-assessment

DeFelice, Alexandra (2010). Cloud Computing: What Accountants Need to Know. Journal of Accountancy, November, 2010. Retrieved on March 1, 2012 from

http://sju.com/documents/cloud_computing_what_accountants_need_to_know.pdf

Dell Corporation (Dell) (2012). Dell Poweredge T110 II. Retrieved on April 8, 2012 from http://configure.us.dell.com/dellstore/config.aspx?oc=bedt5dd&c=us&l=en&s=bsd&cs=04&model_id=poweredge-t110-2&

Digital Business Law Group, P.A. (2012). HIPAA/HITECH Audit. Retrieved on April 12, 2012 from http://www.digitalbusinesslawgroup.com/ps-hipaa-audit.html

Eckerson, Wayne W (2011). Performance Dashboards: Measuring, Monitoring, and Managing Your Business. Hoboken, NJ: Wiley and Sons

Eckstein, Robert, Collier-Brown, David, and Kelly, Peter (1999, November). Using Samba – 4.8 Logging Configuration Options. Retrieved on April 8, 2012 from http://oreilly.com/openbook/samba/book/ch04_08.html

Edge, Jake. Releasing Samba 4. Retrieved on April 8, 2012 from http://lwn.net/Articles/469792/

Edgeblue.com (2012). Blue Coat SG300 Series Appliances. Retrieved on April 9,2012 from http://www.edgeblue.com/SG300.asp

Elson, J. and Cerpa, A (2003, April). RFC 3507 - Internet Content Adaption Protocol (ICAP). Retrieved on March 15, 2012 from http://tools.ietf.org/html/rfc3507

Epic Systems, Inc. (Epic Systems) (2012). Epic: Departments and Ancillaries. Retrieved on March 1, 2012 from http://www.epic.com/software-ancillaries.php

Evolve Healthcare Training (2012). Buy Online Training Courses Now! Retrieved on April 12, 2012 from http://www.ehipaatraining.com/orderpage.htm

Foley, Mary Jo (2010, February 26). Behind the IDC data: Windows still No. 1 in server operating systems. Retrieved on April 8, 2012 from http://www.zdnet.com/blog/microsoft/behind-the-idc-data-windows-still-no-1-in-server-operating-systems/5408

Geisinger Health System (Geisinger) (2012). PowerPoint Presentation on EMR System Implementation. Retrieved on March 1, 2012 from www.academyhealth.org/files/HIT/**Geisinger**%20Slides.pdf

George, Randy (2009, August 1). Rolling Review: Symantec ‘s DLP-9. Retrieved on April 9, 2012 from http://www.informationweek.com/news/security/attacks/218900115

Giglio, Peggy and Ingram, Julie (2012). Critical Features of an EMR System. Retrieved on March 28, 2012 from http://www.defran.com/_pdf/whitepapercriticalfeatures.pdf

Gokavarapu, Nageswararao V. and Banerjee, Shubhendu (2011, March 8). Virtualization Technologies for Agile Software Development. Retrieved on March 8, 2012 from http://public.dhe.ibm.com/software/dw/aix/au-virtualizationagile-pdf.pdf

Google, Inc., (2012). Google Message Encryption and the new HIPAA Legislation. Retrieved on March 1, 2012 from *http://*www.google.com/postini/pdf/hipaa_encryption.pdf

Government Printing Office (GPO) (2009). American Recovery and Reinvestment Act of 2009. Retrieved on March 4, 2012 from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf

Hawthorn, Nigel (2009, November 5). Finding security in the cloud. Retrieved on March 31, 2012 from http://dx.doi.org.libproxy.temple.edu/10.1016/S1361-3723(09)70131-9

Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology (HIT) 75 Fed. Reg 44617.

HIPAA Administrative Simplification. 45 C.F.R. Pt. 160 (2006)

HIPAA Administrative Simplification: Enforcement (2009), 74 Fed. Reg. 56123.

Health Information Technology Standards Panel (HITSP) (2012). About Healthcare Information Technical Panel – Mission, Leadership, History, Retrieved on March 1, 2012 from http://www.hitsp.org/about_hitsp.aspx

Health Information Technology Standards Panel (HITSP) (2009). HITSP Collect and Communicate Security Audit Trail Transaction. Retrieved on February 4, 2012 from http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=3&PrefixNumeric=15

Health Information Technology Standards Panel (HITSP) (2009). HITSP Secure Communication Channel Transaction. Retrieved on February 4, 2012 from http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=3&PrefixNumeric=17

Health Information Technology Standards Panel (HITSP) (2009). HITSP Consistent Time Transaction. Retrieved on February 4, 2012 from

http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=3&PrefixNumeric=16

Health Information Technology Standards Panel (HITSP) (2009). HITSP Entity Identity Assertion Component. Retrieved on February 4, 2012 from http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=19

Health Information Technology Standards Panel (HITSP) (2009). HITSP Nonrepudiation of Origin Component. Retrieved on February 4, 2012 from http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=26

Humboldt University Informatik (2012). Programming the Linksys WRT54GS Broadband Router. Retrieved on March 15, 2012 from http://sarwiki.informatik.hu-berlin.de/Programming_the_Linksys_WRT54GS_Wireless_Broadband_Router

ICSA Labs (2012). About ISCA Labs. Retrieved on April 9, 2012 from https://www.icsalabs.com/about-icsa-labs

ICSA Labs (2012). ICSA Labs Certified Products – Anti-Virus, Windows 7. Retrieved on April 9, 2012 from https://www.icsalabs.com/products?tid%5B%5D=4216&tid_3%5B%5D=4516&.x=14&.y=19

Ipcop.org (2012). IPCop v2.0.0 Administration Manual. Retrieved on April 10, 2012 from http://www.ipcop.org/2.0.0/en/admin/html/

Kangas, Eric, Ph. D. (2012). Gmail – not HIPAA Compliant Email – LuxSci FYI. Retrieved on March 1, 2012 from http://luxsci.com/blog/gmail-not-hipaa-compliant-email.html

Kerberos Consortium (2012). The Role of Kerberos in Modern Information Systems. Retrieved on April 8, 2012 from http://technet.microsoft.com/en-us/library/cc773013(WS.10).aspx

King, Leo (2011, November 22). Nasdaq Out of Date Software Helped Hackers Report. Retrieved on March 28, 2012 from http://www.csoonline.com/article/694804/nasdaq-out-of-date-software-helped-hackers-report

Kukkukk, Gunter (2012, March 7). [Samba] User audit logging. Retrieved on April 8, 2012 from https://lists.samba.org/archive/samba/2012-March/166517.html

Kumar, Sameer and Aldrich, Krista (2010). Overcoming barriers to electronic medical record (EMR) implementation in the US healthcare system: A comparative study. Health Informatics Journal 2010 16: 306. DOI: 10.1177/1460458210380523

Long, Kurt (2011, July). Proactive Defense. Retrieved on April 2, 2012 from http://www.hhnmag.com/hhnmag_app/jsp/articledisplay.jsp?dcrpath=TRUSTEEMAG/Article/data/07JUL2011/1107TRU_aboveboard_PracticalMatters&domain=TRUSTEEMAG

Longwood Systems, Inc. (2012). Longwood Systems, Inc. | Solutions | Electronic Medical Records. Retrieved on April 1, 2012 from http://www.longwoodsystems.com/medicalrecords.html

Marchany, R.C and Tront, J.G. (2002). E-commerce Security Issues. Retrieved on March 31, 2012 from http://dx.doi.org/10.1109/HICSS.2002.994190

McAfee Corporation (McAfee) (2012). Data Sheet – McAfee Endpoint Encryption. Retrieved on April 8, 2012 from http://www.mcafee.com/us/resources/data-sheets/ds-endpoint-encryption.pdf

McAfee (2012). McAfee DLP Prevent. Retrieved on April 9, 2012 from http://www.mcafee.com/us/resources/data-sheets/ds-dlp-prevent.pdf

McAfee Corporation (2012). McAfee Encrypted USB. Retrieved on April 8, 2012 from http://www.mcafee.com/us/resources/data-sheets/ds-encrypted-usb.pdf

McAfee Corporation (2012). McAfee ePolicy Orchestrator System Requirements. Retrieved on April 8, 2012 from http://www.mcafee.com/us/products/epolicy-orchestrator.aspx#=vtab-Requirements

Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule (2010), 75 Fed. Reg. 44314.

Mell, Peter, and Grance, Tim (2009, October 7). Effectively and Securely Using the Cloud Computing Paradigm. Retrieved on March 31, 2012 from http://bing.exp.sis.pitt.edu:8080/webdav/cloud_resources/cloud_computing_112111/cloud-computingNISTpresentation.pdf

MessageLabs, Inc. (MessageLabs) (2012). Configuring Proxy Settings using Group Policy Management. Retrieved on March 15, 2012 from http://images.messagelabs.com/help/en-us/content/web_security_services/configuring_proxy_settings_using_group.htm

Microsoft Corporation (Microsoft). (2010, May 3). Best Practices for BitLocker in Windows 7. Retrieved on March 15, 2012 from http://technet.microsoft.com/en-us/library/dd875532(v=ws.10).aspx#BKMK_gpsettings

Microsoft Corporation (Microsoft) (2012). BitLocker Drive Encryption. Retrieved on April 8, 2012 from http://windows.microsoft.com/en-US/windows7/products/features/bitlocker

Microsoft Corporation (Microsoft). (2011, March 19). Create an SMTP Send Connector. Retrieved on March 15, 2012 from http://technet.microsoft.com/en-us/library/aa997285.aspx

Microsoft Corporation (Microsoft) (2012). Hardware and Software Requirements for SQL Server 2012. Retrieved on April 8, 2012 from http://msdn.microsoft.com/en-us/library/ms143506.aspx

Microsoft Corporation (Microsoft) (2010, March 12). How the Windows Time Service Works. Retrieved on April 8, 2012 from http://technet.microsoft.com/en-us/library/cc773013(WS.10).aspx

Microsoft Corporation (Microsoft) (2010, July 1). How to use Windows Software Update Services to deploy definition updates to computers that are running Windows Defender. Retrieved on March 15, 2012 from http://support.microsoft.com/kb/919772

Microsoft Corporation (Microsoft) (2012). Windows Server 2008 R2 Active Directory Overview. Retrieved on April 8, 2012 from http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory-overview.aspx

Microsoft Corporation (Microsoft) (2012). Windows Small Business Server Overview. Retrieved on March 15, 2012 from http://www.microsoft.com/en-us/server-cloud/Windows-Small-Business-Server/overview.aspx

Microsoft Store (2012). Windows Anytime Upgrade. Retrieved on April 8, 2012 from http://www.microsoftstore.com/store/msstore/list/parentCategoryID.44066700/categoryID.50726200

Microsoft Support (2006, October 31). How to configure Active Directory diagnostic event logging in Windows Server 2003 and Windows 2000 Server. Retrieved on April 8, 2012 from http://support.microsoft.com/kb/314980

Microsoft Technet (2009, October 7). Identify Patches/Hotfixes installed on a computer on a given date. Retrieved on April 8, 2012 from http://gallery.technet.microsoft.com/scriptcenter/5aedad0f-753b-43e8-bd3f-fdbbccb64256

Miller, Robert H., and Sim, Ida (2004, March). Physicians' Use of Electronic Medical Records: Barriers and Solutions. doi: 10.1377/hlthaff.23.2.116 *Health Aff March 2004 vol. 23 no. 2 116-126*

Mohamed, Arif (2009). A History of Cloud Computing. Retrieved on March 6, 2012 from http://www.computerweekly.com/feature/A-history-of-cloud-computing

Nahra, Kirk J. (2008, November/December). HIPAA Security Enforcement is here. Retrieved on April 1, 2012 from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4753677

National Institute of Standards and Technology (NIST) (2012). Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules. Retrieved April 8, 2012 from http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm#1332

NetMarketShare (2012). Top Operating System Share Trend – May 2011 to March 2012. Retrieved on April 8, 2012 from http://www.netmarketshare.com/os-market-share.aspx?qprid=9

Newegg.com (2012). Lexar JumpDrive FireFly 4GB USB 2.0 Flash Drive Model LJDFF4GBASBNA. Retrieved on April 8, 2012 from http://www.newegg.com/Product/Product.aspx?Item=N82E16820191278s

Office of the National Coordinator for Health Information Technology (ONC-HIT) (2012). Reference Grids for Meaningful Use or Standards and Certification Criteria Final Rules. Retrieved from http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3584 on March 1, 2012

Oracle Corporation (2012). Oracle 2012 Technology Price List. Retrieved on April 01, 2012 from http://www.oracle.com/us/corporate/pricing/technology-price-list-070617.pdf

Ott, French (2009). Hand Hygiene Compliance Among Health Care Staff and Student Nurses in a Mental Health Setting. Issues in Mental Health Nursing, 30:702-704. ISSN 0161-2840 print/ 1096-4673 online. DOI: 10.3109/01612840903079223

PFSense Project (pfSense) (2012). pfSense Open Source Firewall Distribution – Hardware Sizing Guidance. Retrieved on March 15, 2012 from http://www.pfsense.org/index.php?option=com_content&task=view&id=52&Itemid=49

Ray, Ramon (2009, June 8). Using Old Computers Does Not Save you Money. Retrieved on April 01, 2012 from http://smallbiztechnology.com/archive/2009/06/using-old-computers-does-not-s.html/

Recovery.gov (2012). The Recovery Act. Retrieved on March 4, 2012 from http://www.recovery.gov/About/Pages/The_Act.aspx

Red Hat Inc. (Red Hat) (2012). 4.4. Configuration Examples. Retrieved on April 8, 2012 from http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Managing_Confined_Services/sect-Managing_Confined_Services-Samba-Configuration_examples.html

Rock, Connie and Stephens, Mike (2008, February). Windows Server 2008 – Planning and Deploying Group Policy. Retrieved on April 8, 2012 from http://www.microsoft.com/download/en/confirmation.aspx?id=22478

Rousskov, Alex (2012). Feature: ICAP (Internet Content Adaption Protocol). Retrieved on April 9, 2012 from http://wiki.squid-cache.org/Features/ICAP

RSA, an EMC Company (RSA) (2012). RSA Data Loss Prevention. Retrieved on March 28, 2012 from http://www.emc.com/security/rsa-data-loss-prevention.htm

Samba.org (2012). What is Samba? Retrieved on April 8, 2012 from http://www.samba.org/samba/what_is_samba.html

Securehq.com (2012). Websense Websense WebSense Security Gateway. Retrieved on April 9, 2012 from http://www.securehq.com/group.wml&groupid=1453

Siemens Corporation (Siemens) (2012). Soarian Integrated Care. Retrieved on April 8, 2012 from http://www.medical.siemens.com/siemens/en_GB/gg_hs_FBAs/files/HIE/SIC_ProductBrochure_e_2006.pdf

Snort.org (2012). About Snort. Retrieved on March 15, 2012 from http://www.snort.org/snort

Snyder, Joel (2012). CSI: Five Critical Questions for NAC. Retrieved on March 8, 2012 from http://www.exclusive-networks.com/downloads/it/documentations/5%20Critical%20questions%20for%20NAC.pdf

Squid-cache.org (2012). Squid: optimizing web delivery. Retrieved on April 9, 2012 from http://www.squid-cache.org/

Stallings, W. (2008) . Computer Security: Principles and Practice. Upper Saddle River, NJ: Pearson Prentice Hall

Stephenson, Peter (2007, November 1). McAfee Data Loss Prevention Appliance. Retrieved on April 9, 2012 from http://www.scmagazine.com/mcafee-data-loss-prevention-appliance/review/1137/

Supremus Group (2012). Covered Entity HIPAA Compliance Tool. Retrieved on March 16, 2012 from http://www.hipaatraining.net/Covered-Entity-HIPAA-Compliance-Tool-less-50employee.htm

Symantec Corporation (Symantec) (2012). PGP Whole Disk Encryption – System Requirements. Retrieved on April 8, 2012 from http://www.symantec.com/products/sysreq.jsp?pcid=pcat_info_risk_comp&pvid=wd_encryption_1

Symantec Corporation (Symantec) (2012). Security and Privacy for Healthcare Providers. Retrieved on March 1, 2012 from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-security_and_privacy_for_healthcare_WP_20934020.en-us.pdf

Symantec Corporation (2012). Symantec Endpoint Encryption Removable Storage Edition. Retrieved on April 8, 2012 from http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-see_removeable_storage_DS_21157418.en-us.pdf

Symantec Corporation (Symantec) (2012). Symantec PGP Whole Disk Encryption – MSRP Per License. Retrieved on April 8, 2012 from http://www.symantec.com/content/en/us/store/volume_pricing/PGP-Whole-Disk-Encryption-081911.pdf

Techotopia.com (2012). Configuring BitLocker Drive Encryption on Windows Server 2003. Retrieved on March 15, 2012 from http://www.techotopia.com/index.php/Configuring_BitLocker_Drive_Encryption_on_Windows_Server_2008

Trend Micro (2012). Worry-free Business Security. Retrieved on March 15, 2012 from http://www.trendmicro.com/cloud-content/us/pdfs/home/brochures/br_worryfree-family.pdf

Touchet BK, Drummond SR, Yates WR: Brief reports: the impact of fear of HIPAA violation on patient care. Psychiatr Serv 2004;55:575–576

Tovino, Stacey A. and Reisz, Cynthia Y. Protecting PHI: Legal Duties of Health Care Lawyers Post-HITECH. Retrieved on April 1, 2012 from http://publish.healthlawyers.org/Events/Programs/Materials/Documents/PHYHHS11/reisz_tovino_including_exhibits_a-b.pdf

TrueCrypt (2012). Frequently Asked Questions. Retrieved on April 8, 2012 from http://www.truecrypt.org/faq

Valdes, I, Kibbe, D.C., Tolleson, G., Kunik, M.E., Petersen, L.A. (2004, February 1). Barriers to Proliferation of Electronic Medical Records. Retrieved on April 1,

2012 from http://www.ingentaconnect.com/content/rmp/ipc/2004/00000012/00000001/art00002#expand/collapse

Venema, Wietse (2012). Postfix TLS Support. Retrieved on March 15, 2012 from http://www.postfix.org/TLS_README.html

Wang, Samuel J., Middleton, Blackford, Prosser, Lisa A., Bardon MD, Christiana G., Spurr, Cynthia D., Carchidi, Patricia J., Kittler, Anne F., Goldszer, Robert C., Fairchild, David G., Sussman, Andrew J., Kuperman, Gilad J., Bates, David W (2003). A cost-benefit analysis of electronic medical records in primary care. The American Journal of medicine, 114(5), 397-403.

Websense Corporation (2012). Websense Web Security: Integrating the Content Gateway component with Third Party Data Loss Prevention Applications. Retrieved on April 9, 2012 from http://www.websense.com/content/support/library/web/v75/wcg_misc/Web_Security_Gateway_DLP_ICAP_Integration.pdf

Whitten, Alma, and Tygar, J.D. (2005). Why Johnny Can't Encrypt – A Usability Evaluation of PGP 5.0. Retrieved on April 8, 2012 from http://www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf

WorldVista Inc. (2012). VistA History. Retrieved on March 1, 2012 from http://worldvista.org/AboutVistA/VistA_History

Zandri, Jason (2009, February 19). Windows 7 Editions Comparison. Retrieved on March 28, 2012 from http://www.petri.co.il/windows-7-editions-comparison.htm

Zhivan, Natalia A. and Diana, Mark L. (2012). U.S. Hospital Efficiency and Adoption of Health Information Technology. Health Care Manag Sci (201) 15:37-37 DOI: 10.1007/s10729-011-9179-2

Appendix A- Cloud-based/Remotely Hosted Security Evaluation Matrix

A – Encryption

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
A100	Emergency Access	Does the organization permit authorized emergency user access to ePHI during an emergency	**§164.312(a)(2)(ii), §170.302(p)**	Yes	Yes
A101	Encryption of data at remote sites	Does the organization allow for encryption of data so that unauthorized personnel at the remote site do not have access to the data?	**45 CFR 160 and 164, §170.302(u),**	Yes	Yes
A102	Encryption of portable media and hard drives	Does the organization encrypt protected health information at risk of being lost on hard drives or removable media such as USB drives or portable hard drives?	**45 CFR 160 and 164**	Yes	Yes
A103	Device and Media Controls	Does the organization have the ability to track the transfer of ePHI onto electronic media that may be able to be removed from the facility, such as USB drives, laptops, or removable hard drives?	**§164.310(d)(1)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
A104	Transmission Security	Does the organization encrypt and decrypt data when exchanging electronic health information using approved security functions as defined by Annex A of NIST FIPS 140-2?	**§164.312(e)(1), §170.302(v), 45 CFR 160 and 164, HITSP/T17**	Yes	Yes
A105	Encryption	Does the organization encrypt electronic health information at rest using approved security functions as defined by Annex A of NIST FIPS 140-2?	**§170.302(u), 45 CFR 160 and 164, HITSP/T16**	Yes	Yes
A106	Integrity	Does the organization implement policies, procedures, and technical controls to ensure that protected health information is not altered or destroyed in an unauthorized manner?	**§164.312(c)(1), §170.302(s), HITSP/T15**	Yes	Yes

B – Technical Policy and Unique User Identification/Access Control					
Control Number	**Control**	**Description**	**Standard(s)**	**Applies to Cloud/ Services Provider**	**Applies to Small/Medium Health Care Organization**
B100	Workstation Logical/Physical Security	Are there physical safeguards to only allow access to ePHI on workstations by authorized users?	**§164.310(c)**	Yes	Yes
B101	Access Control	Does the organization implement policies and procedures for allowing access to those persons or software programs that have been granted access rights?	**§164.312(a)(1)**	Yes	Yes
B102	Unique User Identification	Does the organization assign a unique user name and/or number for tracking user identity when accessing ePHI? Does this extend to system services and/or applications? NOTE: This means that default user accounts or shared accounts cannot be used for accessing ePHI, providing technical support to systems containing it, or running services or shared applications that process it.	**§164.312(a)(2)(i), §170.302(o)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
B103	Audit Controls	Does the organization implement hardware, software, and procedural mechanisms to record and examine activity in systems that contain ePHI?	**§164.312(b), §170.302 (r), HITSP/T15**	Yes	Yes
B104	Person or Entity Authentication	Does the organization implement policies or procedures to verify that a person or entity that wants access to ePHI is who they claim to be?	**§164.312(d), §170.302(t), HITSP/C19**	Yes	Yes
B105	Consistent Time	Does the organization use NTP or SNTP to synchronize time across all computer systems that access PHI?	**HITSP/T16**	Yes	Yes
B106	Non-repudiation/Centralized Authentication	Does the system which contains ePHI use non-repudiation of origin to ensure that whoever enters, changes, or deletes data is who they say they are? I.E. do they use a centralized authentication system, PKI, or similar system such as Active Directory or Kerberos? Do the SSL certificates used provide assertion that the sites are who they say they are?	**HITSP/C26, HITSP/T17, HITSP/T15, HITSP/T16, §164.306(a)(4), §164.308(a)(3)(i)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
B107	Document Updates	Is documentation on systems updated periodically when changes to the environment that affect systems containing protected health information are made?	**§164.316(b)(2)(iii)**	Yes	Yes
C – Proxy Server and Data Loss Prevention					
Control Number	**Control**	**Description**	**Standard(s)**	**Applies to Cloud/ Services Provider**	**Applies to Small/Medium Health Care Organization**
C100	Transmission Security	Does the organization encrypt and decrypt data when exchanging electronic health information using approved security functions as defined by Annex A of NIST FIPS 140-2?	**§164.312(e)(1), §170.302(v), 45 CFR 160 and 164, HITSP/T17**	Yes	Yes
C101	Protection against unauthorized disclosure	Has the organization implemented controls that protect against any reasonably anticipated disclosures?	**§164.306(a)(3), 45 CFR Parts 160 and 164, §170.210(a)(1), §170.210(a)(2)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
C102	Device and Media Controls	Does the organization have the ability to track the transfer of ePHI onto electronic media that may be able to be removed from the facility, such as USB drives, laptops, or removable hard drives?	**§164.310(d)(1)**	Yes	Yes
D – Firewall					
Control Number	**Control**	**Description**	**Standard(s)**	**Applies to Cloud/ Services Provider**	**Applies to Small/Medium Health Care Organization**
D100	Protection against unauthorized disclosure	Has the organization implemented controls that protect against any reasonably anticipated disclosures?	**§164.306(a)(3), 45 CFR Parts 160 and 164, §170.210(a)(1), §170.210(a)(2)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
D101	Physical Safeguards	Does the organization implement policies and procedures to limit physical access to its electronic information systems and their physical facilities, while allowing authorized access?	**§164.310(a)(1)**	Yes	Yes
D102	Integrity	Does the organization implement policies, procedures, and technical controls to ensure that protected health information is not altered or destroyed in an unauthorized manner?	**§164.312(c)(1), §170.302(s), HITSP/T15**	Yes	Yes
E – Antivirus					
Control Number	**Control**	**Description**	**Standard(s)**	**Applies to Cloud/ Services Provider**	**Applies to Small/Medium Health Care Organization**

E100	Integrity	Does the organization implement policies, procedures, and technical controls to ensure that protected health information is not altered or destroyed in an unauthorized manner?	**§164.312(c)(1), §170.302(s), HITSP/T15**	Yes	Yes
E101	Protection against unauthorized disclosure	Has the organization implemented controls that protect against any reasonably anticipated disclosures?	**§164.306(a)(3), 45 CFR Parts 160 and 164, §170.210(a)(1), §170.210(a)(2)**	Yes	Yes
F – Policies, Procedures, Risk/Impact Analysis, and Contracts					
Control Number	**Control**	**Description**	**Standard(s)**	**Applies to Cloud/ Services Provider**	**Applies to Small/Medium Health Care Organization**
F100	ONC-ATCB Certification	Is the Cloud/Remotely-hosted EMR Solution ONC-ATCB Certified by CCHIT for the current year?	**CCHIT ONC-ATCB Certification Controls**	Yes	
F101	Service Level Agreement	Does the Cloud Services provider have a service level agreement that defines acceptable levels of service interruption, downtime, and notification of adverse events?	**AICPA Service Organization Controls**	Yes	

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F102	Service Organization Controls 2 Report	Does the hosting organization or data center have a Service Organization Controls 2 report that documents the implementation effectiveness of privacy and security controls?	**AICPA Service Organization Controls, §164.306(a)(2), §164.308(a)(ii)(A), 164.308(a)(ii)(B), 164.306(a)(3), 45 CFR Parts 160 and 164, §170.210(a)(1), §170.210(a)(2), §164.306(a)(4), §164.308(a)(3)(i), §164.308(a)(4)(i), §164.308(a)(5)(i), §164.308(a)(ii)(D)**	Yes	Yes, if they are a service provider.
F103	Security Risk Analysis	Has the organization undergone a security risk analysis to determine the most likely threats?	**§164.306(a)(2), §164.308(a)(ii)(A)**	Yes	Yes
F104	Security Risk Mitigation	Has the organization implemented reasonable and appropriate countermeasures to the risks identified in the risk assessment?	**§164.308(a)(ii)(B)**	Yes	Yes
F105	Workforce Security Compliance Standards	Has the organization taken steps to ensure that its workforce complies with HIPAA security standards?	**§164.306(a)(4), §164.308(a)(3)(i)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F106	Workforce Security	Has the organization implemented policies and procedures to ensure that all workforce members have access to protected health information that require it?	**§164.308(a)(3)(i)**	Yes	Yes
F107	Workforce Sanctions	Has the organization implemented sanctions on workforce members who do not comply with security policies and procedures?	**§164.308(a)(ii)(C)**	Yes	Yes
F108	Information Access Management	Has the organization implemented policies and procedure for authorizing access to protected health information consistent with acceptable usage standards?	**§164.308(a)(4)(i)**	Yes	Yes
F109	Security awareness and training	Has the organization implemented a security awareness and training program for all organization members, including management?	**§164.308(a)(5)(i)**	Yes	Yes
F110	Audit Log Review	Has the organization implemented procedures to review records of information system activity, including audit logs, access reports, and incident tracking reports on a regular basis?	**§164.308(a)(ii)(D)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F111	Assigned Security Responsibility	Has a security official who is responsible for the required policies and procedures been identified?	**§164.308(a)(2)**	Yes	Yes
F112	Security Incident Procedures	Has the organization implemented policies and procedures to address security incidents, including response, mitigation, and documentation of incidents and their outcomes?	**§164.308(a)(6)(i)**	Yes	Yes
F113	Contingency Plan	Has the organization established and implemented policies and procedures for responding to emergencies or other unnatural occurrences, including backups, a disaster recovery plan, and an emergency mode operations plan?	**§164.308(a)(7)(i)**	Yes	Yes
F114	Business Impact Analysis	Has the organization performed a Business Impact Analysis to predict the consequences of a disruption in business operations and gather the information required to develop recovery strategies?	**Required by §164.308(a)(7)(i)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F115	Periodic Evaluation	Does the organization perform periodic technical and non-technical re-evaluations of environmental and operational changes that can affect the security of protected health information?	**§164.308(a)(8)(i)**	Yes	Yes
F116	Business Associates	Does the organization ensure that its business associates that deal with protected health information appropriately protect the data?	**§164.308(b)(1)**	Yes	Yes
F117	Physical Safeguards	Does the organization implement policies and procedures to limit physical access to its electronic information systems and their physical facilities, while allowing authorized access?	**§164.310(a)(1)**	Yes	Yes
F118	Workstation Use	Are their policies and procedures that govern proper workstation usage?	**§164.310(b)**	Yes	Yes
F119	Workstation Physical Security	Are their policies and procedures that govern the physical placement of a workstation and its surroundings to protect ePHI?	**§164.310(b)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F120	Device and Media Controls	Does the organization have policies and procedures that govern the receipt and removal of physical or electronic media that contains ePHI into and out of the facility?	**§164.310(d)(1)**	Yes	Yes
F121	Disposal Procedures	Does the organization have policies and procedures governing the final disposition of ePHI, and the hardware and media which may store it?	**§164.310(d)(2)(i), 45 CFR 160 and 164**	Yes	Yes
F122	Media re-use	Does the organization have policies and procedures governing the removal of ePHI from electronic media before it is made available for re-use	**§164.310(d)(2)(ii), 45 CFR 160 and 164**	Yes	Yes
F123	Business Associate Agreements	Do the Business Associate agreements stipulate that business associates will implement the proper administrative, physical, and technical safeguards which will reasonable and appropriately protect the confidentiality, integrity, and availability of protected health information?	**§164.314(a)(1)(i), §164.314(a)(2)(i)(A)**	Yes	Yes
F124	Subcontractors	Do the Business Associate agreements stipulate that subcontractors will also take reasonable and appropriate safeguards to protect ePHI?	**§164.314(a)(2)(i)(B)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F125	Reporting of incidents	Do the Business Associate agreements require contractors or subcontractors to report any security incidents to the covered entity of which they are aware?	**§164.314(a)(2)(i)(C)**	Yes	Yes
F126	Termination of contract	Do the Business Associate agreements give the right to terminate the contract if the covered entity determines that they are in violation of the contract?	**§164.314(a)(2)(i)(D)**	Yes	Yes
F127	Government Organization	If the covered entity and its business associate are government organizations, is there a memorandum of understanding that stipulates that data will be protected as per the HIPAA Security Rule?	**§164.314(ii)(A)(1)**	Yes	Yes
F128	Good Faith	If a business associate is required by law to collect information and cannot meet security requirements as per the HIPAA Security Rule, it can continue to provide services provided it attempts in good faith to comply	**§164.314(ii)(B)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F129	Termination Clause Omission	A covered entity may omit the authorization of contract termination if it is in conflict with the statutory obligations of the covered entity or its business associate	**§164.314(ii)(C)**	Yes	Yes
F130	Group Health Plans	If the business associate is a group health plan, and unless the information is used for marketing, plan management, or enrollment status purposes, the plan must appropriately safeguard and protect ePHI	**§164.314(b)(1)**	Yes	Yes
F131	Policies and Procedures	Are organizational policies and procedures maintained in electronic and written form?	**§164.316(a)**	Yes	Yes
F132	Policies and Procedure Implementation	Has the organization implemented reasonable and appropriate policies and procedures to comply with the HIPAA Security Rule?	**§164.316(a)**	Yes	Yes
F133	Documentation	Does the organization maintain written records of assessments, actions, or incidents that occur?	**§164.316(b)(ii)**	Yes	Yes
F134	Anti-overlook policies	Does the organization not permit or excuse actions that violate HIPAA requirements?	**§164.316(a)**	Yes	Yes

Control Number	Control	Description	Standard(s)	Applies to Cloud/ Services Provider	Applies to Small/Medium Health Care Organization
F135	Document Retention	Does the organization have document retention policies that retain organizational policies, procedures, and documentation for a period of at least six years from creation or last effective date, whichever is later?	**§164.316(b)(2)(i)**	Yes	Yes
F136	Document Updates	Is documentation on systems updated periodically when changes to the environment that affect systems containing protected health information are made?	**§164.316(b)(2)(iii)**	Yes	Yes

Appendix B - Glossary

ACS: Affiliated Computer Services

AD: Active Directory

AICPA: American Institute of Certified Public Accountants

ARRA: American Reinvestment and Recovery Act

BIA: Business Impact Analysis

CCHIT: Certification Commission for Health Information Technology

CIFS: Common Internet File System

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CMS: Center for Medicare and Medicaid Services

CPA: Certified Public Accountant

DLP: Data Loss Prevention

EACH: EHR Alternative Certification for Healthcare providers

EMR: Electronic Medical Record

EHR: Electronic Health Record

ePHI: Electronic Protected Health Information

FIPS: Federal Information Processing Standards

GPO: Government Printing Office

HHS: Department of Health and Human Services

HIPAA: Health Information Portability and Accountability Act

HITECH Act: Health Information Technology for Economic and Clinical Health Act

HITSP: Healthcare Information Technology Standards Panel

ICAP: Internet Content Adaption Protocol

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

NAC: Network Access Control

NIST: National Institute of Standards and Technology

NTP: Network Time Protocol

ONC-ATCB: Office of the National Coordinator – Authorized Testing and Certification Body

PGP: Pretty Good Privacy

PHI: Protected Health Information

SAS: Statement on Auditing Standards

SMB: Server Message Block

SOC: Service Operational Controls

USB: Universal Serial Bus

Temple University

Improving Healthcare Provider Information Security Through the Implementation of Financial Systems Structures and Controls

August 2014

TEMPLE UNIVERSITY

Improving Healthcare Provider Information Security Through the Implementation of Financial Systems Structures and Controls

SGM 5182 Independent Study Project

Parker, Mitchell

8/5/2014

EXECUTIVE SUMMARY

Two of the most critical industries in the United States are finance and healthcare. Finance is responsible for the efficient transferal of monetary value across the world. Healthcare ensures the well-being of the American population. One salient item that both have in common is that both industries are subject to a myriad of regulations and guidance to ensure secure and efficient operations. However, that is where the similarities end. While both have no shortage of checks and balances, finance is much more well-organized and governed.

The purpose of this paper is to illustrate the differences between the approaches to Information Security in finance and healthcare. The centralized model in finance will be explained. The main entity responsible for ensuring security, which is the Center for Medicare and Medicaid Services, will have its role and regulations explained. The issues with the current model in healthcare will be explored in detail. Reasons why this current situation exists will then be explained thoroughly. These reasons will include structural, legal, and situational, and financial analysis of healthcare providers' current state. A SWOT analysis will be used to discuss the current situations with healthcare information security in the context of policies, procedures, and effective communication. Means by which the hospital and healthcare industry can improve this situation will then be explored through the use of a similar enterprise risk management structure as finance, and the use of Healthcare Information Exchanges (HIEs) as a strategic tool. A risk/feasibility analysis of this potential solution and some of its pitfalls will be explored. The overall goal is to demonstrate the application of Information Security controls from the Financial Services community can potentially lead to efficiencies and a reduction of fraud, waste, and abuse with healthcare providers.

CENTRALIZED FINANCE INFORMATION SECURITY MODEL

Applicable financial institutions, under Section 501(b) of the Graham-Leach Bliley Act (GLBA), are required to establish appropriate standards to insure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to their security and integrity, and to protect against unauthorized access or use that could lead to customer harm (106th Congress, 1999). These aforementioned financial institutions include federally chartered banks, members of the Federal Reserve systems, federal and state branches of international banks, banks insured by the Federal Deposit Insurance Corporation (FDIC), savings associations insured by the FDIC, credit unions insured by the National Credit Union Association, brokers and dealers insured by the Securities and Exchange Commission, investment advisors, and insurance companies (106th Congress, 1999).

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to establish principles, standards, and report forms for the federal examination of financial institutions (FFIEC, 2014). They are given such power by their member agencies, which include the Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), the National Credit Union Association (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (FFIEC, 2014). They are also empowered to make recommendations to promote uniformity in the supervision of financial institutions (FFIEC, 2014). In addition, they also provide training for state examiners upon request (FFIEC, 2014). The FFIEC trains and certifies financial examiners using the same training programs across the Financial Services industry (FFIEC, 2014).

As part of these standards, the FFIEC has developed the FFIEC IT Examination HandBook InfoBase (FFIEC, 2014). This handbook provides standards, expectations, and guidance on Audit, Business Continuity, Development and Acquisition, Electronic Banking, Information Security,

Management, Operations, Outsourcing Technology and vendor solutions, Retail Payment Systems, Supervision of Technology Service Providers, and Wholesale Payment Systems (FFIEC, 2014). This Infobase is the one playbook used by federal (and many state) auditors and inspectors as a reference platform. Enforcement actions on violations of these standards and guidance in the Infobase are the responsibility of the member agencies (FFIEC, 2014).

According to the FFIEC's IT Handbook Infobase, which is the standard financial services guidance, development of the Information Security Program for applicable financial institutions is the responsibility of organizational management (FFIEC, 2014). The Board of Directors is responsible for approving it (FFIEC, 2014). The Board, according to the Graham-Leach Billey Act, is also responsible for overseeing the development, implementation, and maintenance of the program (FFIEC, 2014). It is also responsible for assigning the specific responsibility for its implementation (FFIEC, 2014). The Board is also responsible for approving the written information security policies and overall program at least annually (FFIEC, 2014). This approach of top-down assignment of responsibility starting with the Board of Directors, certified examiners with a standardized curriculum, communication of requirements to all stakeholders, Homeland Security directives directing organizations to share information, and a large centralized Information Sharing community show a strong approach to Information Security in finance.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) was established in 1999 in response to 1998's Presidential Directive 63, and revised by Homeland Security Presidential Directive 7 (FS-ISAC, 2014). These directives mandated that private and public sector organizations share information about physical and cyber security threats and vulnerabilities (FS-ISAC, 2014). The New York State Department of Financial Services, in their May 2014 Report on Cyber Security in the Banking Sector, recommended that all New York State-chartered depository financial institutions become members of FS-ISAC (NYS DFS, 2014). The reason for this is because the rapid pace of change has made

it more critical that these institutions use the information-sharing and analysis resources available to them (NYS DFS, 2014). The Commonwealth of Massachusetts' Division of Banks has issued similar guidance to all of their state-chartered banks on June 18, 2014 (Commonwealth of Massachusetts, 2014). As of 2011, over 4,000 institutions belong to the FS-ISAC (FS-ISAC, 2011). This is the latest membership count available.

Furthermore, this approach to Information Security governance in Finance has led to more developed Enterprise Risk Management programs in this industry (J of Healthcare Risk Mgmt, 2005). Enterprise Risk Management, which provides a global view of risk throughout the organization, requires the support of the board and CEO. Since they are held accountable under GLBA, the maturity of Enterprise Risk Management programs can be seen as a possible outgrowth of it.

HEALTHCARE INFORMATION SECURITY MODEL

The Center for Medicare and Medicaid Services (CMS), under the guidance of their Office for Civil Rights (OCR), requires applicable organizations, known as Covered Entities, to be compliant with the HIPAA Privacy Rule, and the HIPAA Security Rule (CMS, 2014). Covered Entities are health care providers that transmit information electronically in connection with a transaction for which the Department of Health and Human Services has adopted a standard (CMS, 2014). HIPAA does require health plans and health care clearinghouses, which are organizations that process nonstandard transactions and information into standard ones, to comply (CMS, 2014). The transactions include claims and encounter information, payment and remittance advice, claims status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits, and premium payment (CMS, 2014). This can be widely interpreted to mean that anyone who submits a claim using a standard format, or uses a tool which does so, is subject to the provisions of the HIPAA Privacy Rule and HIPAA Security Rule.

Business Associates, which are third parties that conduct business on behalf of covered entities, are also subject to the provisions of HIPAA. They are required to only use the Protected Health Information for only the intended purposes of the covered entity (CMS, 2014). They are required to safeguard the information, and will assist the covered entity in complying with some of their duties under the HIPAA Privacy Rule (CMS, 2014). In addition, they are required to notify the covered entity in the case of a breach, and are required to remediate it (CMS, 2014). This requires that the covered entity get satisfactory assurances in writing, specifically in the form of a contract or agreement, to ensure this (CMS, 2014).

There are four main rule sets for HIPAA. The first is the HIPAA Privacy Rule, defined as 45 CFR Part 160 and subparts A and E of 45 CFR Part 164 (CMS, 2014). The HIPAA Security Rule is defined as 45

CFR Part 160 and subparts A and C of 45 CFR Part 164 (CMS, 2014). The Breach Notification Rule is defined as 45 CFR Part 164, subparts 400-414 (CMS, 2014). The HITECH Act, which promotes the adoption and meaningful use of health information technology, was adopted in 2009. It establishes four categories of violations and levels of culpability. It also establishes four corresponding penalty tiers, and sets a maximum penalty of $1.5 million for all violations of an identical provision (CMS, 2014).

There is no corresponding training program or set of standards for all covered entities and business associates to follow. These entities are expected to interpret and apply the rules by themselves. In an interview with Dave Snyder, Chief Information Security Leader for Independence Blue Cross, on June 30th, 2014, he indicated that the stances of CMS and the Office of the National Coordinator are to allow the industry to police itself (Snyder, 2014). CMS has not agreed upon a security framework (Snyder, 2014). CMS does provide training for providers on HIPAA in conjunction with Medscape, one of the more popular medical web sites (Medscape, 2014). However, there is no evidence of a comprehensive training program for the HIPAA Privacy Rule, HIPAA Security Rule, Breach Notification Rule, or HITECH Act.

In December of 2013, eHealth Initiative, a non-profit policy and advocacy group based out of Washington DC, held an event called "Integrating Privacy & Security into Organizational Strategy & Culture". During this event, representatives from both the Office of Civil Rights (OCR) and Office of the National Coordinator (ONC) spoke. The representative from the Office of Civil Rights indicated that there was a need to implement necessary training and education for Business Associates to make them aware of HIPAA rules (eHealthInitiative, 2014). She also stated that healthcare organizations are ultimately responsible for making their business associates aware of their privacy and security obligations (eHealthInitiative, 2014). Advisory Board participants indicated that the HIPAA Security Rule as challenging and in need of clarity (eHealth Initiative, 2014).

The current model in healthcare is to provide the regulations with little corresponding training. There is little clarity being given to the HIPAA Security Rule, which is causing consternation with a large group of providers. Representatives of the Mayo Clinic, Children's Hospital of Philadelphia, PriceWaterhouseCoopers, HITRUST, United Healthcare, Cooper Health, and Merck were present at this meeting (eHealth Initiative, 2014). These entities all expressed difficulty with complying with rules in need of clarity.

The HIPAA Security Rule requires that organizations train their workforces on the Information Security Rule (AHIMA, 2014). The American Health Information Management Association, AHIMA, developed a training guide which covers the organizational requirements for training. They indicate that as part of the HITECH Act, CMS has made an individual available in each regional HHS office to provide training and education about everyone's rights and responsibilities under the HIPAA Privacy and Security rules (AHIMA, 2014). There are 10 regional offices for the entire United States. This means that there are 10 people that provide this training for tens of thousands of affected providers.

Unlike the financial industry, there is no guidance given on implementation. CMS published their internal 2010 System Security Procedure, which is available from their web site (CMS, 2010). Their own security plan gives ultimate authority for Information Security to the Chief Information Officer, not the Chief Information Security Officer (CMS, 2010). They also make security training the responsibility of the business owner in their Roles & Responsibilities Matrix (CMS, 2010). This is a disjointed structure that can lead to wildly differing communication about security responsibilities due to no centralized Information Security training resources. The Business Owner does not have the requisite training in Information Security, and the CISO does in their matrix (CMS, 2010).

The disjoint approach in Information Security given by CMS' own Information Security plan corresponds with their current approaches with training outside agencies. The rules and regulations are

there to follow, but there is little, if any, centralized security guidance given to customers, be they internal or external.

ISSUES WITH HEALTHCARE MODEL

There are three major parts of the commerce system. There are the financial services providers, such as banks and lenders. There are the producers of goods and services that customers utilize. Finally, there are the consumers of both financial services and the producers of goods and services. Out of these three, only one of them has tight Information Security regulations, financial services. Only Financial Services has a comprehensive monitoring program enforced by government regulatory standards.

While there are Payment Card Industry (PCI) Information Security Standards for merchants that process credit cards, those controls only apply to the environments that handle them (PCI SSC, 2013). The latest PCI 3.0 standard does emphasize continual monitoring and a robust computing infrastructure, but does not require it for the entire computing environment (PCI SSC, 2013).

According to the National Institute of Standards and Technology (NIST), Information Security can be defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Kissel, 2013). The definition of fraud, from the Association of Certified Fraud Examiners, is that it can encompass any crime for gain that uses deception as its principal modus operandus (ACFE, 2014).

Health care fraud, according to the Wex legal dictionary, is a type of white-collar crime that involves the filing of dishonest health care claims in order to turn a profit (Wex, 2014). It can involve the providing of false information, misuse of legitimate information, billing for unneeded services, or altering of medical information (Wex, 2014). Information security is relevant to health care fraud because Information Security involves the protection of information and information systems from misuse. Health care fraud is a misuse of legitimate information and information systems to commit

crime. The issue present is that there is a significant amount of health care fraud, and that the current enforcement mechanisms as they relate to information security are not capable of dealing with the situation.

Estimates of the cost of health care fraud vary wildly. The aforementioned Wex legal dictionary estimates that 10 cents of every dollar spent on health care goes toward paying for fraudulent health care claims (Wex, 2014). Berwick and Hackbarth, in their paper Eliminating Waste in US Health Care, estimated that fraud and abuse accounted for between $82 billion and $272 billion in wasteful spending in 2011 (Berwick and Hackbarth, 2012). The Association of Certified Fraud Examiners (ACFE) indicated that 6.7% of reported fraud claims came from health care. T.R. Goldman, in the policy brief Eliminating Fraud and Abuse, from the journal Health Affairs, had several different figures. The first, from CMS themselves, indicated that Medicare and Medicaid made $65 billion in improper federal payments in fiscal year 2010 (Goldman, 2012). When improper payments made by states were included, that raised the total by $10 billion (Goldman, 2012). His interpretation of the Berwick and Hackbarth study estimated that fraud and abuse contributed as much as $98 billion to Medicare and Medicaid spending in 2011 (Goldman, 2012). For the purposes of this paper, the estimation of fraud will be between $75 to $98 billion dollars yearly.

In 2012, Healthcare and related services had a 17.2% share of the US Gross Domestic Product (GDP) (Lassman et al., 2014). That is $2.8 trillion dollars in spending on healthcare in the United States in 2012. Financial Services and Insurance companies, according to the US Department of Commerce, had a 7.9% share of US GDP, with an estimated spend of $1.24 trillion dollars in financial services.

The 2013 LexisNexis True Cost of Fraud Study indicated that retailers had lost an estimated 0.54% of revenue to fraud (LexisNexis, 2013). Kroll Advisory Solutions, in the Global Advisory Report, Annual Edition 2012/13, indicated that the average revenue loss from fraud was 1.1% (Kroll Advisory

Solutions, 2013). The estimation of fraud in health care is between 2.68% and 3.5% of overall spending estimating $75 to $98 billion dollars of fraud and $2.8 trillion of overall spending.

This is a significantly higher amount of fraud, by percentage, than the average. Information from health care systems, and the systems themselves, are being misused to commit fraud at a significantly higher rate than the national average. Due to the system and information misuse, this can be construed as both Information Security and Fraud issues.

HIPAA has two major components related to fraud mitigation. The first is that the HIPAA act itself established and funded a program to combat fraud and abuse committed against all health plans, both public and private (USDOJ, 2014). The second is that the HIPAA Security Rule, 45CFR § 164.308 (a)(ii)(D), requires an Information System Activity Review (CMS, 2014). Covered Entities are required to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports (CMS, 2014).

The HITECH Act, in addition, provides financial incentives for organizations to adopt Electronic Medical Record (EMR) technology under the Meaningful Use program (CMS, 2014). This means that providers and hospitals who adopt this technology, which means that they have full electronic records and data sets, can get incentive money back from CMS for demonstrating effective use in their environment.

The Patient Privacy and Affordable Care Act (PPACA), more colloquially referred to as "Obamacare", Public Law 111-148, March 23, 2010, has several more provisions to detect and combat against fraud. Section 6401 calls for enhanced provider screening, including licensing checks, criminal background checks, unscheduled and unannounced site visits, and any other screening deemed appropriate (111th Congress, 2010). Section 6401 also requires organizations to disclose any direct or indirect affiliations with providers that may have been previously sanctioned (111th Congress, 2010).

They have the right to deny enrollment to any organization that poses an undue risk of fraud, waste, or abuse (111th Congress, 2010).

Section 6401 also allows CMS to adjust payments of providers of services and suppliers for past due obligations (111th Congress, 2010). This means that any organization that has outstanding obligations to CMS will just have them taken out of receivables. This also means that providers, who typically run very low profit margins, run the risk of losing revenue instead of negotiating a payment plan with CMS. Section 6401(a)(3) of the PPACA also establishes the requirement that providers and suppliers have a compliance program in place (111th Congress, 2010).

Section 6402, the Enhanced Medicare and Medicaid Program Integrity Provisions, amends Part A of title XI of the Social Security Act (42 USC 1301) to add a new section, 1128J, which establishes, at a minimum, a data repository for all claims submitted to Medicare and Medicaid (Title XVIII and XIX), State Children's Health Insurance (Title XXI), Health-related programs from the Veterans' Administration, Department of Defense, Federal old-age and survivors insurance trust fund and federal disability insurance trust fund (Title II), and Indian Health Service data (111th Congress, 2010). Medicare and Medicaid data has priority for inclusion (111th Congress, 2010). The purpose of this is to collect data for fraud, waste, and abuse (111th Congress, 2010). This also gives the Attorney General full access to said claims data for the purpose of examining it for fraud, waste, and abuse (111th Congress, 2010).

Section 6407 requires a face to face encounter with a patient before certifying eligibility for home health services or durable medical equipment under the Medicare program (111th Congress, 2010). This was put in to guard against people abusing this program to sell unnecessary equipment to patients that may not need it. Section 6504 requires providers to report an expanded set of data elements to detect fraud and abuse (111th Congress, 2010).

The provisions within PPACA have good intentions. However, there are several factors which preclude their adoption in a way that benefit hospitals. These options will be looked at to show how economic factors and other initiatives such as ICD-10, Meaningful Use, HCAHPS (Patient Satisfaction), and Recovery Audit Contractor (RAC) audits may impact the ability of organizations to comply with the anti-fraud stipulations in HIPAA, HITECH, and PPACA.

First of all, hospitals are low-margin businesses. According to the American Hospital Association, in a survey of member community hospitals by Avalere Health of 2012 economic data, the average total hospital margin is 7.8% (AHA, 2014). 21.3% of surveyed hospitals have negative total margins (AHA, 2014). 25.9% of surveyed hospitals have negative operating margins (AHA, 2014). The percentage change of the Employment Cost Index for hospitals is 2.8% (AHA, 2014).

According to the 2013 edition of AHA Hospital Statistics, out of the nearly 5,000 nonfederal, short-term general community hospitals in the United States, the average revenue is $151.9 million, and the average profit per hospital is $10.7 million (Herman, 2013). This indicates an average profit margin of 7.04%. One other item of note is that the median average age of plant in 2012 is 10.2 years, which is up from 8.2 in 1992 (AHA, 2013).

The cost of ICD-10 implementation, which is the International Code of Diseases, Version 10, requires providers to implement new codes for billing. According to a cost study initiated by the American Medical Association and conducted by Nachimson Advisors, it will cost between $2 and $8 million dollars to implement ICD-10 in a large physician practice (AMA, 2014). This is a significant cost for practices to bear, and the study includes the loss of productivity and payment disruption in it (AMA, 2014). In addition, the AMA notes that claims denial rates could increase 100 to 200 percent in the initial stages of ICD-10 adoption (AMA, 2014). This is a major financial risk for hospitals that has long-reaching implications.

Adoption of Electronic Medical Records, which is required for Meaningful Use, has several high costs as well. An analysis by Dr. RJ Teufel of the Medical University of South Carolina in the Journal of Academic Pediatrics in 2012 analyzed 4,605,454 weighted discharges by hospitals (Acad Pediatr., 2012). The analysis indicated that EMR was associated with a 7% average greater cost per case (Acad Pediatr., 2012). In addition, hospitals that do not adopt and demonstrate meaningful usage of EMR systems will only receive 75 percent of the adjustment to their Inpatient Prospective Payment System reimbursements in year 1 (CMS, 2014). In year 2, they will receive 50 percent, and year 3 onward, only 25 percent of the increases (CMS, 2014).

Meaningful Use incentive payments only cover 20 to 25 percent of the overall implementation costs required to meet the requirements (Sinno, Gandhi, and Gamble, 2011). This is because there are multiple costs to replace ancillary systems that provide a complete picture of care (Sinno, Gandhi, and Gamble, 2011). Sinno, Gandhi, and Gamble also indicate that the cost of implementing an EMR and the required initiatives competes with the limited capital dollars needed for strategic facility decisions, purchase of biomedical equipment, and ancillary clinical systems (Sinno, Gandhi, and Gamble, 2011). Sinno, Gandhi, and Gamble also cite a short-term artificial increase in labor costs due to the demand for skilled clinical analysts exceeding supply (Sinno, Gandhi, and Gamble, 2011).

To protect the Meaningful Use money, hospitals are required to conduct a security risk analysis and implement updates during each reporting period (CMS, 2014). The penalties for not doing so including returning part or all of the Meaningful Use money received (CMS, 2014). Under PPACA, CMS can just take the money out of future receivables (111th Congress, 2010). The 2014 AHA Chartbook, for their set of data, indicated that Medicare accounted for 39.7% of costs by payer type for community hospitals (AHA, 2014). A sudden deduction of margins would cause many hospitals in that data set to have a serious financial event. A risk analysis from a CPA firm such as PriceWaterhouseCoopers can cost

over $100,000 per year. Hospitals need to reassign or hire skilled security staff to ensure that the security requirements are met. Even if Meaningful Use is met, the costs of doing so offset the anticipated benefit.

The Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) is a program that surveys patients based on patient satisfaction (Clark, 2012). Hospitals that score poorly on HCAPS surveys can be expected to be penalized 0.4% to 1% on their Medicare payments (Clark, 2012). This potential reduction in revenue may cause hospitals to redirect their focus onto patient satisfaction, since there is a potential loss of revenue there.

In 2005, CMS started a program called the Recovery Audit Program. Third-party Recovery Audit Contractors (RAC) review claims with supporting documentation (CMS, 2014). They determine whether or not the services were necessary, and can issue denials of claims (CMS, 2014). These contractors receive commissions based on the amount of money recovered for Medicare (CMS, 2014). They only can review the past three years of claims (CMS, 2014). They can also audit up to 400 records in a 45-day period (CMS, 2012). Handling this number of audits can cause an extra administrative burden for providers. The Philadelphia Inquirer, in their July 27, 2014 edition, profiled Fox Rehab, a Philadelphia-area company that had to lay off 62 office workers and has had a 15 percent cut in their Medicare reimbursements for outpatient physical therapy (Brubaker, 2014). The American Hospital Association has also weighed in and determined that the RAC program causes urgent and critical problems with additional resources being required to appeal claims (AHA, 2014). They also note that the RAC system is so overloaded that it takes two years to see an administrative law judge (AHA, 2014). The RAC program in itself, while a good idea, causes providers significant overhead and negatively affects their ability to focus on providing care.

There are several other costs to consider as well. Accurately checking the data for fraud and breaches of privacy requires staff and a lot of analysis. In an interview with MedCityNews, Dr. Bimal Desai, the Chief Medical Information Officer for Children's Hospital of Philadelphia, indicated several important facts. He gave an example of how many rows of audit data needed to be reviewed for a patient. For an inpatient with a two week hospital stay, there were over 100,000 rows of data (Baum, 2014). Random audits of 100 patient medical records at other hospitals, in his experience, take one to two full-time employees two weeks (Baum, 2014). He further indicates a large disconnect between what hospitals must do, and what they can actually do (Baum, 2014). Additionally, he indicates that the access logs of EMRs were never designed to detect breaches (Baum, 2014).

The American Hospital Association, in their 2012 AHA Annual Survey, indicates that there were 5,723 registered hospitals in the US (AHA, 2014). There were 36,156,245 admissions to these hospitals in 2012 (AHA, 2014). This averages out to approximately 6,318 admissions per year per hospital. To be able to examine the set of medical records to a 95% confidence level with a 5% confidence interval would require sampling at least 363 records. To be able to examine the set of medical records to a 99% confidence level with a 5% confidence interval would require sampling at least 603 records. If an average hospital examines 1,200 records per year, they are examining their records to at least a 99% confidence level with a 5% confidence interval.

However, dedicating at least two employees to this task would cost approximately $200,000 a year for an average hospital, and significantly more for a much larger facility. Automated tools such as FairWarning may be required for large multi-hospital environments that have complex data integration. Reporting may need to be built in, costing a hospital significantly more money.

With all these additional costs, there is no guidance given on how to implement these systems. What is being done now is a "best guess" estimate given the rules. Information Security and Fraud

Protection is not a fiscal priority for hospitals. Evidence shows that the impact of ICD-10, Meaningful Use, HCAHPS, RAC Audits, and ongoing risk assessments and monitoring are the priorities for keeping hospitals fiscally sound. The AHA's survey also showed the average age of physical plant equipment increasing over the past 20 years, which also shows a potential trend of spending less there to make up for other revenue shortfalls. Since Medicare is a 34.9% chunk of revenue for hospitals in the AHA sample set, affecting that revenue stream may have detrimental effects when the average profit margin of a hospital is 7%. Many hospitals simply do not have the revenue stream to effectively implement Information Security programs to the satisfaction of all of the proscribed government regulations due to competition with other priorities.

HIPAA and HITECH are currently being enforced by direct reporting to the Office of Civil Rights, voluntary reporting, or by compliance reviews (CMS, 2014) (CMS, 2014). CMS has admitted that the HIPAA Security Rule is in need of clarity (eHealth Initiative, 2014). They have also put the onus on training of business associates on the providers themselves (eHealth Initiative, 2014). This has led to a situation where organizations are not even clear on what the requirements are, or what they need to comply to. In this situation, organizations will do the minimum necessary work.

To be able to accurately match patients across multiple organizations, and to be able to use those data sets to prevent fraud, there needs to be a universal identifier. However, in 1998, political and privacy concerns caused Congress to enact legislation as part of the Omnibus Appropriations Act that prevents the Department of Health and Human Services from doing so (AHIMA, 2011). Section 6402 of PPACA establishes a data warehouse for collecting data on all claims to examine them for fraud, waste, and abuse. Medicare and Medicaid still use the Social Security Number for claims (AHIMA, 2011). The act of establishing a data warehouse with all Medicare and Medicaid claims is a potential security risk because the Social Security Number can be used for fraud. Aggregating that data together across

multiple providers and entities at a national level provides significant risk. Adding to this, CMS will have the ability to examine all claims from an organization. Even if an organization has examined their medical records to a 99% confidence level, there runs the risk of them detecting fraud or misuse that a well-designed monitoring process may not.

Adding to this, the Office of the National Coordinator has not issued guidelines on patient matching identification yet (eHealth Initiative, 2014). Patient matching is still performed in silos, which leads to privacy risks when payors and providers exchange information (eHealth Intiative, 2014). ONC's Patient Matching Initiative is still in formative discussion stages (Stevens and Black, 2014). This is an outstanding risk in that CMS does not even have the current capability to implement a data warehouse and match patients accurately, and is collecting claims data for one.

The current issues with the healthcare model are that there is a lot of policy in effect, but no centralized guidance and education on it. There is also little clarity on the HIPAA Security Rule. Both HITECH and PPACA add additional checks and balances on top. However, there are provisions of both that cannot be accurately enforced. Due to the lack of clarity, healthcare Information Security is not centrally organized or well-organized, as opposed to the centralized governance model in Financial Services. The current economic situation of hospitals implementing ICD-10, Meaningful Use, Electronic Medical Records, RAC audit programs, and HCACPS with a lower or negative operating margin also leads to less than optimal enforcement of the rules and organizations doing the minimum necessary work. Fraud detection, while mandated as part of PPACA, presents a privacy risk in itself because there is no national healthcare identifier. In addition, the matching algorithms to match patients across organizations accurately have not been vetted yet, meaning that CMS is not even capable of realizing the benefits.

While there is a significant amount of fraud, the low operating margins, resource-intensive RAC audits, HCAHPS, emphasis on changing medical billing and coding via ICD-10, Meaningful Use, and Electronic Medical Records effectively stretch provider resources to the point where fraud detection is not feasible and may cause more economic harm than good. The provider resource issues caused by the RAC program to recover $9 billion show that CMS is not working well with them to resolve fraud and information security issues.

SWOT Analysis of Healthcare Provider Information Security

After describing the issues with Information Security in healthcare, a SWOT analysis of the current situation for these programs providers needs to be performed. This illustrates where resources need to be focused and strategic alternatives developed to help resolve the current situation.

Strengths:	Weaknesses:
1. Organizations have to comply with HIPAA. 2. Meaningful Use payments require Information Security risk assessments.	1. The HIPAA Security Rule is unclear. 2. HITECH Act record review requirements constrain resources.
Opportunities:	Threats:
1. Resource constraints will cause organizations to think strategically to save money. 2. Health Information Exchanges (HIE), which require interoperability between organizations, are required as part of Stage II Meaningful Use (HealthIT, 2014). 3. Proper organizational alignment will allow Information Security to have more opportunities for influence and action.	1. RAC Audits have caused significant resource constraints. 2. ICD-10 implementation has caused resource scarcity. 3. Electronic Medical Records and the corresponding labor cost cause further resource scarcity. 4. Ancillary systems to support EMR cause resource constraints. 5. Aging hospital physical plant requires attention. 6. Section 6401 of PPACA allows Medicare to deduct penalties from receivables. 7. Section 6402 allows CMS to build a data warehouse of all claims to mine for auditing purposes. 8. CMS has not effectively communicated security requirements. 9. CMS is attempting to enforce policies that do not have a sound technical backing (Section 6402 of PPACA). 10. No national identifier for patients, which makes matching more difficult. 11. No proven patient matching algorithms in use by CMS. 12. CMS does have an effective structure for Information Security management.

STRATEGIC ALIGNMENT OF RISK MANAGEMENT

Healthcare providers face multiple external threats to their organization. Fraud, ambiguity and uncertainty on the part of CMS, multiple competing initiatives such as ICD-10 and Meaningful Use, and RAC audits all present clear and present threats to the net income of an organization. There are several ways by which healthcare organizations can strategically realign themselves to resolve these issues. The purpose of these realignments is to realign the organization to better handle ambiguity and uncertainty. Since there is no guidance given on organizational structure, audits, or organizational form like in Financial Services, the ambiguity and uncertainty is magnified.

To provide alignment of resources, the organizational components that handle compliance, privacy, fraud detection, Information Security, Risk Management, and Regulatory Affairs need to report under Enterprise Risk Management. One of the major issues, as Vincent Oliva posited for the insurance industry, was as that industry faced ever-growing regulatory challenges, companies needed to develop an enterprise risk management strategy as information was kept in silos (Oliva, 2007). Generally, in healthcare, Compliance and Privacy report to the Legal department. Information Security usually reports to the Chief Information Officer (Otisik, 2011). Regulatory Affairs usually reports to the Chief Medical Officer. Fraud Detection falls to either Information Security or Compliance. These are all silos separated by executives that do not have dealing with risk as their primary goal.

In this posited new structure, these departments would report to a Chief Risk Officer. The purpose of the Chief Risk Officer is to provide a C-level view of Enterprise Risk Management and a global perspective of the interrelationship of all risks in the organization (J of Healthcare Risk Mgmt, 2005). A 2011 survey of 400 companies found that 79 percent of banks had an enterprise risk management system, as opposed to 67 percent of all companies surveyed (Crosman, 2011). This may be due directly

to GLBA legislation and FFIEC/member agency enforcement of it. The Chief Risk Officer would report to both the Board of Directors and the CEO. Having the CRO report to them brings a strategic view of organizational risk to decisions with great gravity.

With the advent of Electronic Medical Records, the operations of the healthcare provider are captured in sophisticated computer systems, in addition to their human capital. This means that the above parties are now involved in a technology-heavy organization, and need to use these EMR systems as an integral part of their jobs. With the numerous external threats caused by RAC Audits, multiple system implementations driven by incentives and regulation, PPACA, and capital requirements, there cannot be silos anymore. Integrating these groups together means that a more flexible organization can respond to issues. As organizations become more reliant upon EMRs, their visibility and risk grows. Decisions on configuration and workflow changes in EMRs now resonate across the organization. An organization that can appropriately assess, plan, and mitigate risk in these systems need to be able to negotiate across it effectively both at the C-level and operationally.

An example of this is in fraud management. Instead of having multiple departments working toward separate solutions for fraud management, Information Security, Risk Management, Compliance, and Privacy could work together toward an integrated solution to address enterprise risk. The same resources that work on RAC audits could be utilized to proactively analyze claims to identify “at risk” claims and address any potential issues. This same team could also work on access reviews and potential pitfalls.

Separating out Information Security from the CIO and moving it under Enterprise Risk Management provides additional checks and balances for critical information systems projects such as ICD-10 and EMRs. Healthcare organizations are required to conduct risk assessments as part of Meaningful Use. Having a separate team consisting of Information Security, Compliance, Privacy, and

Regulatory Affairs under the CRO conducting the risk assessments would remove any conflicts on the part of the CIO, and give an impartial view of the risks to the CEO and Board. As information systems become more critical to the survival of healthcare providers, the need for an enterprise risk management approach to gauge and measure risk becomes prevalent.

Due to a lack of scarce skilled resources, a high degree of ambiguity and uncertainty, and a growing dependence on technology, Enterprise Risk Management should be the governing structure for Information Security, Compliance, and Regulatory initiatives. There needs to be management of risk across the enterprise, and the removal of “silos” of information.

HEALTH INFORMATION EXCHANGE STRATEGY

Health Information Exchanges (HIEs), which are a requirement of Stage 2 Meaningful Use, are a method (and exchange) by which healthcare providers can access and share patient information with each other (HealthIT.gov, 2014). This allows providers to access information from each other without having to directly interface systems. While some HIEs have had significant financial issues, and many have closed (Beck and Wilde Mathews, 2014), there are still significant benefits to be had through integration. The integration from HIEs can parallel the advantages used by information sharing in the Financial Services Information Sharing and Analysis Center (FS-ISAC).

On August 4th, 2014, two of the largest insurers in the state of California, WellPoint and Anthem Blue Cross announced plans to fund the California Integrated Data Exchange, or Cal Index (Beck and Wilde Mathews, 2014). This HIE will contain data on over 9 million patients. Both of these companies are investing in initiatives that tie health provider reimbursements to quality and efficiency methods (Beck and Wilde Mathews, 2014). Having the full patient records available will allow providers to potentially cut out waste and reduce duplication (Beck and Wilde Mathews, 2014). It will also allow providers to see the whole picture when it comes to patients. Since the payors and providers are involved, and there is financial gain to be had through reimbursements, organizations are more likely to participate.

One of the largest problems with HIEs is matching patients across organizations. This takes dedicated resources, as CMS has not figured out how to algorithmically match patients yet (eHealth Initiative, 2014). Utilizing regional HIEs that have payors and providers participating can provide a much smaller data set which can be more easily matched. Patients who have their records transferred and matched via HIE can be flagged by Enterprise Risk Management for audit review. The issues discovered

in the audit review process can be utilized to provide better patient matching and continual improvement.

HIEs can also be used to run fraud-detection algorithms on a very large data set. This will allow them to detect fraud patterns across a region that would not be detectable in one provider, such as patients that utilize multiple providers and pharmacies to purchase painkillers. It would also be able to detect multiple orders of durable medical equipment, unnecessary multiple treatments, and excessive orders. Potential fraudulent patients can be flagged using these algorithms as well.

Accountable Care Organizations are groups of doctors, hospitals, and other providers that come together voluntarily to give highly coordinated care to patients (CMS, 2014). The goal of this coordination of care is to make sure that patients get the right care they need, without unnecessary duplication of services and with the prevention of errors (CMS, 2014). HIEs provide a vehicle for all the participants in an ACO to coordinate together to provide a higher standard of care and have one place to look for all of a patient's data. This shared savings model can present incentive for ACOs to participate.

The issue of free riding in HIEs can be mitigated by several factors. First, as Beck and Wilde Mathews indicated, by providing reimbursements based on quality and efficiency to providers for using the HIE to cut out waste and duplication. Secondly, by providing the ability to mine HIE data for fraud, regional patterns of fraud can be detected and potentially remediated. Third, Accountable Care Organizations presents an opportunity for multiple providers and hospitals to integrate data sets and financially benefit from information sharing. Fourth, by keeping the HIE at a regional level, a degree of Clan Control can be achieved, which is a use of social characteristics, such as shared values, commitment, traditions, and beliefs to control behavior (Daft, 2007). Clan Control is critical when ambiguity and uncertainty are high (Daft, 2007). Fifth, there is the potential for establishing HIE-level identities for patients that do not use the Social Security Number. While there is no funding for a

national-level patient identifier due to the Omnibus Rule, there is no such specification at the regional level. This can allow providers, once a patient is matched, to carry the identity across multiples. This can also benefit ACOs by allowing them to use that identity in the care process, and more easily identify their patients. This can lead to further efficiencies, both financial and in quality of care.

Information Security can also be better achieved in HIEs by establishing clear standards for data security for participants. By enforcing continual verified security as a condition of participation, the shared risk of data sharing can be mitigated. This can also allow for organizations to share information on how to better secure systems for the purpose of data interchange. Information Security information sharing can be facilitated through HIEs in conjunction with other ISACs, Infragard, the Department of Homeland Security, and other federal and regional agencies.

HIEs, when used properly, can mitigate fraud, provide efficiencies in care, and provide financial benefit. When used at the regional level, they can be used to improve the quality of care within that region. When used with ACOs, they are a necessary tool to properly share information and gain efficiencies. With PPACA, CMS will be establishing their own data warehouse of claims. However, due to the lack of a good matching process, this is not going to happen yet. In the words of Jennifer Covich Bordenick, CEO of eHealth Initiative, in the August 5th, 2014 edition of the Wall Street Journal, "It's up to the private sector to step in and take over where the federal government left off" (Beck and Wilde Mathews, 2014). It's to the advantage of providers and payors to reduce fraud, waste, and abuse on their own and develop efficiencies to deal with RAC audits and the eventual data mining that will occur. The current situation with CMS not even having an organizational structure conducive to Information Security only exacerbates the situation.

RISK ANALYSIS

Information Security and Fraud in healthcare is a prevalent issue. These issues stem from a systemic lack of control across healthcare. There is significant risk no matter what decision is made due to the volatility and uncertainty of the environment. The risks of not implementing the strategic recommendations will therefore be discussed.

The risk of not implementing an Enterprise Risk Management program to manage risk across the organization means that healthcare organizations will not be able to structure themselves like the financial community, and will not be able to effectively manage and communicate risk throughout the organization. In addition, the board and CEO will not be held accountable for risk. This also means that the efficiencies gained by centralizing the silos in the organization that manage risk will not be realized. Organizations will not be able to manage fraud, waste, and abuse as efficiently, and the current situation will continue to exist.

The risk of not implementing a Healthcare Information Exchange (HIE) strategy means that providers will be missing opportunities to reduce fraud, waste, and abuse through information sharing and analysis. There will also be missed opportunities for financial enrichment through participation in Accountable Care Organizations. Finally, the organization will not be able to meet criteria for Meaningful Use, meaning that potential revenue loss from the incentive money for implementing an Electronic Medical Record system will occur.

Due to the uncertain structure and implementation of security controls by CMS, including RAC audits, lack of clarity on the HIPAA Security Rule, and the complexity of compliance, strategic actions need to be taken to ensure that healthcare provider organizations are able to adequately identify, prioritize, and manage risk. The current situation, as-is, will lead to a continuation of the status quo. CMS is not structured or able to manage their risk, as evidenced by the enmity and resource drain

caused by the RAC program. The structure and organization in their own Security Plan also indicates an organization that does not train its own workforce well, and does not have good communication. Providers need to manage their own risk at an enterprise level, and utilize regional-level resources to assist in doing so due to these factors.

CONCLUSION

Financial Services provides an excellent structural model for ensuring accountability. Their model of centralized policy development and education has led to a simple, centralized model governed by the FFIEC which trains the industry how to identify, prioritize, and manage Information Security risks. This has led to a lower occurrence of fraud in the Financial Services industry. Their model holds the board of directors and management accountable for the establishment, monitoring, and governance of an Information Security Program.

Healthcare, however, is not as organized. There are multiple policies and procedures governing Information Security, specifically the HIPAA Security Rule, HITECH, and PPACA ("Obamacare") . By the admission of their own staff, they have not done a credible job in communication of them to their customers. Their own internal Security Plan and communications also have poor structure and do not provide for the CISO to run a training or communication program, pushing the responsibility on the business owners.

The Medicare program, in particular, suffers from an estimated $75 to $98 billion dollars a year in fraud, waste, and abuse. However, the main recipients of the benefits of this program, hospitals, average 7 percent profit margins. CMS, as part of HIPAA, HITECH, and PPACA, has placed stringent anti-fraud controls on providers. In addition to these controls, they have asked for several high-price and high-resource commitments from organizations in exchange for continued payments, including ICD-10, Meaningful Use, Electronic Medical Records, HCAHPS, and compliance with Recovery Audit Contractor audits. These initiatives compete with Information Security and reducing fraud, waste, and abuse. There is an impact to the bottom line, and the required level of security may not be achievable given limited resources.

What healthcare providers need to bring improvement to their environments and achieve benefits while reducing fraud, waste, and abuse are two key items. First, healthcare providers need to adopt Enterprise Risk Management like many Financial companies have, and unify the resources responsible for it in Risk Management, Information Security, Compliance, Privacy, and Regulatory Affairs into one central organization headed by a Chief Risk Officer that identifies, prioritizes, and manages risk at an enterprise level. This enterprise risk organization would also achieve economies of scale by sharing formerly disparate resources across one Risk organization.

Secondly, providers need to look at Healthcare Information Exchanges as something more than just a requirement for Meaningful Use. There are several opportunities to reduce duplication of tests, enter into incentive programs with payors, and use regional HIEs as a platform for managing ACOs. There are also additional chances to use anti-fraud algorithms against a larger data set to detect potential fraud, waste, and abuse. There are also opportunities to use HIEs to establish regional-level identities for patients, thereby improving patient matching at the grassroots level. They can also replicate the Financial Services Information Sharing and Analysis Center (FS-ISAC) structure at a regional level and improve Information Security communication across healthcare.

There is room for improvement in healthcare provider Information Security. However, due to the uncertain internal and external communication and enforcement of the rules by CMS, it is incumbent upon the providers to improve their own internal risk management structures to more efficiently manage risk internally. It is also incumbent for providers, payors, and ACOs to work together to mitigate shared risks and reduce fraud, waste, and abuse on their own, without waiting for CMS to do so.

REFERENCES

106th Congress (1999, November 12). Public Law 106-102-Nov. 12, 1999. Graham-Leach Bliley Act. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf on August 2, 2014.

111th Congress (2010, March 23). Public Law 111-148-March 23, 2010. The Patient Protection and Affordable Care Act. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf on August 2, 2014.

Acad Pediatr. 2012 Sep-Oct;12(5):429-35. Hospital electronic medical record use and cost of inpatient pediatric care. doi: 10.1016/j.acap.2012.06.004. Epub 2012 Jul 21.

AHIMA. "Limiting the Use of the Social Security Number in Healthcare." *Journal of AHIMA* 82, no.6 (June 2011): 52-56.

American Health Information Management Association (AHIMA) (2014). HIPAA Privacy and Security Training (Updated). Retrieved on August 2, 2014 from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048509.hcsp?dDocName=bok1_048509

American Hospital Association (AHA) (2014). Chartbook – Trends Affecting Hospitals and Health Systems. Retrieved on August 3, 2014 from http://www.aha.org/research/reports/tw/chartbook/ch4.shtml

American Hospital Association (AHA) (2014). Fast Facts on US Hospitals. Retrieved August 3, 2014 from http://www.aha.org/research/rc/stat-studies/fast-facts.shtml

American Hospital Association (AHA) (2014). RAC Auditing Reform is Essential to Fix Urgent, Critical Problems. Retrieved on August 4, 2014 from http://www.aha.org/content/14/issuebrief-rac.pdf

American Medical Association (AMA) (2014, February 12). ICD-10 Cost Estimates Increased for Most Physicians. Retrieved on August 3, 2014 from http://www.ama-assn.org/ama/pub/news/news/2014/2014-02-12-icd10-cost-estimates-increased-for-most-physicians.page

Association of Certified Fraud Examiners (ACFE) (2014). What is Fraud?. Retrieved on August 3, 2014 from http://www.acfe.com/fraud-101.aspx

Association of Certified Fraud Examiners (ACFE) (2012). 2012 Report to Nations. Retrieved on August 3, 2014 from http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

Baum, Stephanie (2014, July 23). Children's Hospital CMIO turns entrepreneur to more rapidly detect patient data breaches. Retrieved on August 3, 2014 from http://medcitynews.com/2014/07/childrens-hospital-cmio-turns-entrepreneur-to-prevent-patient-data-breaches/

Beck, Melinda and Wilde Mathews, Anna (2014, August 5). Two Insurers to Pool Medical Records in California. Retrieved on August 5, 2014 from http://online.wsj.com/articles/two-insurers-to-pool-medical-records-in-california-1407211305

Berwick, Donald and Hackbarth, Andrew. Eliminating Waste in US Health Care. doi:10.1001 /jama.2012.362

Brubaker, Harold (2014, July 27). Costs of expanded audits aimed at Medicare fraud hit health-care firms. Retrieved on August 4, 2014 from http://articles.philly.com/2014-07-28/business/52094475_1_medicare-fraud-medicare-spending-medicaid-services

Center for Medicare and Medicaid Services (CMS) (2014). Accountable Care Organizations. Retrieved from http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/ on August 5, 2014

Center for Medicare and Medicaid Services (CMS) (2014). Breach Notification Rule. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html on August 2, 2014.

Center for Medicare and Medicaid Services (CMS) (2014). Business Associates. Retrieved on August 2, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

Center for Medicare and Medicaid Services (CMS) (2010, August 31). CMS System Security Plan (SSP) Procedure. Retrieved on August 2, 2014 from http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/SSP_Procedure.pdf

Center for Medicare and Medicaid Services (CMS) (2014, May). Eligible Hospital and Critical Access Hospital Meaningful Use Core Measures. Retrieved on August 3, 2014 from http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/14_Protect_Electronic_Health_Information.pdf

Center for Medicare and Medicaid Services (CMS) (2014). Health Information Privacy – For Covered Entities and Business Associates. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html on August 2, 2014.

Center for Medicare and Medicaid Services (CMS) (2014). HITECH Act Enforcement Interim Final Rule. Retrieved on August 2, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

Center for Medicare and Medicaid Services (CMS) (2014). How CMS Enforces the HIPAA Privacy and Security Rules. Retrieved on August 3, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html

Center for Medicare and Medicaid Services (CMS) (2014). Instructions for Submitting Notice of a Breach to the Secretary. Retrieved on August 3, 2014 from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Center for Medicare and Medicaid Services (CMS) (2014). Payment Adjustment for Medicare Subsection (d) Eligible Hospitals. Retrieved on August 3, 2014 from http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/PaymentAdj_HardshipExcepTipsheetforHospitals.pdf

Center for Medicare and Medicaid Services (CMS) (2012, December 18). RAC Program Myths. Retrieved on August 4, 2014 from http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Recovery-Audit-Program/Downloads/RAC-Program-Myths-12-18-12.pdf

Center for Medicare and Medicaid Services (CMS) (2014). The Privacy Rule. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/ on August 2, 2014.

Center for Medicare and Medicaid Services (CMS) (2014). The Recovery Audit Program and Medicare. Retrieved on August 4, 2014 from http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Recovery-Audit-Program/Downloads/The-Recovery-Audit-Program-and-Medicare-Slides-051313.pdf

Center for Medicare and Medicaid Services (CMS) (2014). The Security Rule. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/ on August 2, 2014.

Center for Medicare and Medicaid Services (CMS) (2014). Transactions & Code Sets Standards. Retrieved on August 2, 2014 from http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/TransactionCodeSetsStands/index.html?redirect=/transactioncodesetsstands/05_codesets.asp

Clark, Cheryl (2012, December 12). Higher Readmission Penalties Linked to Low HCAHPS Scores. Retrieved on August 3, 2014 from http://www.healthleadersmedia.com/page-1/FIN-287372/Higher-Readmission-Penalties-Linked-to-Low-HCAHPS-Scores

Commonwealth of Massachusetts, Division of Banks (2014, June 18). TO THE CHIEF EXECUTIVE OFFICER OF THE FINANCIAL INSTITUTION ADDRESSED. Retrieved on August 2, 2014 from http://www.mass.gov/ocabr/docs/dob/cybersecurityresources.pdf

Crosman, P. (2011, August 1). Chief Risk Officers Rule. *Bank Technology News*, *24*(08), 15. Retrieved from

http://go.galegroup.com/ps/i.do?id=GALE%7CA263061422&v=2.1&u=temple_main&it=r&p=ITOF&sw=w&asid=04c65f72dd8dc7b74344dccad399b75c

Daft, Richard (2007). Organization Theory and Design, 9th Edition. Mason, OH: Thomson Higher Education, 2007.

eHealthInitiative (2014, February 26). Integrating Privacy & Security into Organizational Strategy & Culture. Retrieved on August 2, 2014 from http://www.ehidc.org/resource-center/event-summaries/view_document/374-event-summary-integrating-privacy-security-into-organizational-strategy-culture

Federal Financial Institutions Examination Council (FFIEC) (2014). About the FFIEC. Retrieved on August 2, 2014 from http://www.ffiec.gov/about.htm

Federal Financial Institutions Examination Council (FFIEC) (2014). Enforcement Actions and Orders. Retrieved on August 2, 2014 from http://www.ffiec.gov/enforcement.htm

Federal Financial Institutions Examination Council (FFIEC) (2014). Information Security. Retrieved on August 2, 2014 from http://ithandbook.ffiec.gov/it-booklets/management/it-risk-management-process/it-controls-implementation/information-security.aspx

Federal Financial Institutions Examination Council (FFIEC) (2014). IT Booklets. Retrieved on August 2, 2014 from http://ithandbook.ffiec.gov/it-booklets.aspx

Financial Services Information Sharing and Awareness Center (FS-ISAC) (2014). About FS-ISAC. Retrieved on August 2, 2014 from https://www.fsisac.com/about

Financial Services Information Sharing and Awareness Center (FS-ISAC) (2011). Overview of the FS-ISAC. Retrieved on August 2, 2014 from https://www.fsisac.com/~fsisacki/sites/default/files/FS-ISAC_Overview_2011_05_09.pdf

Goldman, T.R. Eliminating Fraud and Abuse. Retrieved on August 3, 2014 from http://www.healthaffairs.org/healthpolicybriefs/brief.php?brief_id=72

HealthIT.gov (2014). Health Information Exchange (HIE). Retrieved on August 4, 2014 from http://www.healthit.gov/HIE

Herman, Bob (2013, February 4). 13 Statistics on Hospital Profit and Revenue in 2011. Retrieved on August 3, 2014 from http://www.beckershospitalreview.com/finance/13-statistics-on-hospital-profit-and-revenue-in-2011.html

(2005), Part Three: The role of the chief risk officer (CRO). J of Healthcare Risk Mgmt, 25: 19–24. doi: 10.1002/jhrm.5600250407

Kissel, Richard (2013, May). Glossary of Key Information Security Terms. http://dx.doi.org/10.6028/NIST.IR.7298r2

Kroll Advisory Solutions (2013). Global Fraud Report Annual Report 2012/13. Retrieved on August 3, 2014 from http://www.kroll.com/library/krl_fraudreport2012-13.pdf

Lassman, David; Hartman, Micah; Washington, Benjamin; et al (2014, May). National Health Spending In 2012: Rate Of Health Spending Growth Remained Low For The Fourth Consecutive Year. HEALTH AFFAIRS Volume: 33 Issue: 5 Pages: 815-822 Published: MAY 2014

LexisNexis, Inc. (2013). 2013 True Cost of Fraud Study. Retrieved on August 3, 2014 from http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf

Medscape (2014). Protecting Patients' Rights. Retrieved on August 2, 2014 from http://www.medscape.org/sites/advances/patients-rights

New York State Department of Financial Services. Report on Cyber Security in the Banking Sector. Retrieved from http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf on August 2, 2014.

Otisik, Jon (2011, March 31). To Whom Should the CISO Report? Retrieved on August 5, 2014 from http://www.networkworld.com/article/2228899/cisco-subnet/to-whom-should-the-ciso-report-.html

Payment Card Industry Security Standards Council, LLC (PCI SSC) (2013, November). PCI DSS 3.0. Retrieved on August 2, 2014 from https://www.pcisecuritystandards.org/security_standards/documents.php

Sinno, Michael, Gandhi MD, Snehal, and Gamble, Molly (2011, April 28). 8 Problems Surrounding Meaningful Use. Retrieved on August 3, 2014 from http://www.beckershospitalreview.com/healthcare-information-technology/8-problems-surrounding-meaningful-use.html

Stevens, Lee, and Black, Kate. Patient Matching Findings Released. Retrieved on August 3, 2014 from http://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/patient-matching-findings-released/

United States Department of Commerce (Commerce) (2014). The Financial Services Industry in the United States. Retrieved on August 2, 2014 from http://selectusa.commerce.gov/industry-snapshots/financial-services-industry-united-states

United States Department of Justice (USDOJ) (2014). 978 Health Care Fraud and Abuse Control Program and Guidelines. Retrieved on August 3, 2014 from http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00978.htm#statement

Vincent Oliva, Financial Services Research Leader, Industry,Advisory Services. (2007). Take risk management and compliance to the next level -- as insurers face increasingly onerous regulatory compliance demands, they should make enterprise risk management a high priority and consider

appointing chief risk officers. *Insurance & Technology,32*(2), 32. Retrieved from http://search.proquest.com/docview/229288658?accountid=14270

Wex Legal Dictionary (2014). Healthcare Fraud. Retrieved on August 3, 2014 from http://www.law.cornell.edu/wex/healthcare_fraud

APPENDIX D.9
WATER & WASTEWATER COMMITTEE

WATER & WASTEWATER COMMITTEE STRATEGIC PLAN

Chair: John Lucas | Co-Chair: Jon Weirick

September 2018
Indiana Executive Council on Cybersecurity

Water & Wastewater Committee Plan

Contents

Committee Members **4**
Introduction **6**
Executive Summary **8**
Research **10**
Deliverable: Cyber Contact **13**
General Information 13
Implementation Plan 15
Evaluation Methodology 19
Deliverable: Cyber Risk Model (Plan) **21**
General Information 21
Implementation Plan 23
Evaluation Methodology 27
Deliverable: Risk Tool **29**
General Information 29
Implementation Plan 31
Evaluation Methodology 34
Deliverable: Training Plan **36**
General Information 36
Implementation Plan 38
Evaluation Methodology 42
Deliverable: Cyber Plan Template **44**
General Information 44
Implementation Plan 45
Evaluation Methodology 49
Supporting Documentation **51**
IECC Water and Wastewater Committee Cybersecurity Plan Template 52

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
John Lucas	Citizens Energy Group	Vice President, IT, Officer	Chair	Voting
Jon Weirick	City Utilities Engineering, Fort Wayne, IN	Senior Program Manager	Co-Chair	Advisory
Steve Berube	Citizens Energy Group	Manager, Water System Control and Planning	Full Time	Voting
Cliff Campbell	Campbell Consulting, LLC	President	Full Time	Voting
Duane Gilles	Evansville Water and Sewer Utility	Water Distribution Manager	Full Time	Voting
Martin Wessler	Wessler Engineering	Chairman & CEO	Full Time	Voting
Jaimie Foreman	City of Carmel	Drinking Water Regulatory Compliance Administrator	Full Time	Voting
Connie Justice	IUPUI	Director of Cybersecurity Education and Experiential Learning	Full Time	Voting
Douglas Brock	Indiana American Water	Vice President of Operations	As Needed	Non-voting
Brian Rockensuess	Indiana Department of Environmental Management	Chief of Staff	As Needed	Non-voting
Travis Goodwin	Indiana Department of Environmental Management	Security and Counter Terrorism Coordinator	As Needed	Non-voting
Sarah Freeman	IN Utility Regulatory Commission	Commissioner	As Needed	Non-voting
Michelle Funk	IURC	Sr. Utility Analyst	As Needed	Non-voting
Jim Huston	IURC	Commissioner	As Needed	Non-voting
James Haley	City of Fort Wayne	CIO, City of Fort Wayne	As Needed	Non-voting

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - The Water/Wastewater committee conducted research in the following area:
    - Water companies / cybersecurity contact
    - Training for water companies on cybersecurity
    - Funding / legislative options for cybersecurity for water/wastewater companies

- **Research Findings**
  - Lack of contact information on cyber contacts at water companies within Indiana.
  - No risk assessments of cyber capabilities for water companies within Indiana.
  - Lack of understanding and knowledge of existing training for water company personnel.
  - No current regulations for cybersecurity for water companies.

- **Committee Deliverables**
  - Establish Water / Wastewater Cyber Contact with Indiana Department of Environmental Management (IDEM)
  - Cyber Risk Model (Plan)
  - Cyber Risk Tool
  - Training Plan
  - Cyber Security Plan Template for Senate Enrolled Act 362

- **Additional Notes**
  - [No Response]

- **References**
  - [No Response]

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. The Indiana American Water Works Association (AWWA) has provided training via the AWWA website.
    b. We created and ran the Indiana Crit-Ex exercises in 2015.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Small to mid-size water/wastewater utilities with internet access to their Supervisory Control and Data Acquisition (SCADA) systems.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Funding for cyber programs for small to mid-size water/wastewater utilities.
    b. Training on cybersecurity.
    c. Establishing the need for cybersecurity as a high priority compared to infrastructure upgrades.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. National Institute of Standards and Technology (NIST) cybersecurity standard, and the President's Executive Order on cybersecurity. Asset management plan and Cyber Security Plan through SEA 362.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Indiana Crit-Ex After Action Review

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. AWWA Articles/papers
    b. NIST

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Using the AWWA.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Annual cyber training.
    b. Practical cyber training at Muscatatuck.
    c. Federal and/or State financial support for cybersecurity improvements at small and mid-size water and wastewater facilities.
    d. State standards for cybersecurity.
    e. Established and automated cybersecurity risk model.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. Local cyber training
    b. Web-based training
    c. Local government support/awareness of the need for improved cyber

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. There are approximately 500 water companies in Indiana. There are currently no cybersecurity personnel.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. Crit-Ex; Cyber Gym; grow the corporate headquarters in Indiana. This creates the need for cybersecurity companies.

12. **What are your communication protocols in a cyber emergency?**
    a. Protocols vary by utility

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. Best practices should include risk-based templates for evaluating cyber risks based off of the NIST.

Deliverable: Cyber Contacts

Deliverable: Cyber Contact

General Information

1. **What is the deliverable?**
    a. The deliverable will be a cybersecurity contact list for water and wastewater organizations. The list will be in the form of a database that will be regularly updated with contacts specific to each organization's cybersecurity initiatives. This database will work in concert with existing databases that houses additional information for the individual organizations business structure. An added field will complement the focused contact information that exists and provides a direct contact for cyber-related information. The Safe Drinking Water Information System (SDWIS) contains information about public water systems managed by the Indiana Department of Environmental Management (IDEM) will be modified to include the added field for the 'SC' – SCADA Contact.

2. **What is the status of this deliverable?**
    a. In-progress; 50% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The result will be a regularly updated database of cybersecurity contacts for the water / wastewater organizations in the state. The database will be managed and updated at regular intervals by the organizations through the existing update process by IDEM. This contact will alleviate specific focused information to the correct individual of each organization.

6. **What metric or measurement will be used to define success?**
    a. Database establishes a field for cybersecurity contacts. Cybersecurity contacts are updated by the individual organizations of medium and large operators.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. State organizations like IDEM, Department of Homeland Security (DHS), Indiana Utility Regulatory Commission (IURC), and Indiana State Police (ISP) will have the right contact for cybersecurity-related information sharing.
    b. Other industry organizations like Indiana's Water/Wastewater Agency Response Network (InWARN), AWWA, Indiana Rural Water, and Indiana Water Environment Association (IWEA) will also be able to information share using the database.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. IDEM will manage the database.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None at this time.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IDEM

12. **Who should be main lead of this deliverable?**
    a. Travis Goodwin

13. **What are the expected challenges to completing this deliverable?**
    a. Timely updates by the individual organizations will be required to supply the contact information.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Modify IDEM SDWIS Database to include new field	IDEM / Travis Goodwin	100	November 2017	IDEM completed database modifications.
Request organizations to submit 'SC'to IDEM for updates	IDEM	100	January 2018	Requests made to organizations. Awareness shared by partnering organizations INWarn, AWWA, Indiana Rural Water
Update database upon receipt of information	IDEM	20	2019	IDEM recently completed the regular update prior to inclusion of the 'SC'. Next regular update cycle anticipated to have better return.

Resources and Budget

15. Will staff be required to complete this deliverable? No.

a. No (see question 16)

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Database maintenance	Database exists and team to complete. Additional field with minimal additional effort required to complete.	10 hours of database configuration.	2 minutes per field update (550 organizations)	IDEM operations		

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. State organizations like IDEM, DHS, IURC, and ISP will have the right contact for cyber security- related information sharing.
b. Other industry organizations like InWARN, AWWA, Indiana Rural Water, IWEA will also be able to information share using the database.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable will expedite information sharing with the appropriate subject matter expert. Information could be critical information, education, and awareness specific to Indiana's water and wastewater sector.
b. Benefits also include supporting organizations will have the right individual to share information with and reach out for information that may support other organizations.

19. What is the risk or cost of not completing this deliverable?

a. Cost avoidance by organizations creating their own contact list and time saved by having the information available to pertinent parties. Not completing the deliverable will continue the challenge of identifying the right contact for cybersecurity in the water and wastewater sector.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Database configuration and usage of the database available to supporting organizations as well as the state for expedited information. Success will be to have the 'SC' field completed for 95% of community water systems serving over a population of 3,301 or more people.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. New York Department of Health, Division of Environmental Health Protection

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Completion of the database is dependent on community water systems submitting contact information. Regular updates will be required for usefulness.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Ongoing support is already managed through IDEM and its current entry into the existing SDWIS database.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. IDEM – Travis Goodwin and Brian Rockensuess

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All sectors could use for information sharing. A contact database for other sectors could be created where applicable

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. State organizations: IDEM, IDHS, IURC, and ISP.
b. Other industry organizations: InWARN, AWWA, Indiana Rural Water, IWEA

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No
b. Critical contact information should not be shared. IDEM should manage contact information requests specific to critical infrastructure.
c. Reference Indiana Code (IC) 5-14-3, specifically as the disclosure relates to sections:
    i. IC 5-14-4(b)(19)(L)
    ii. IC 5-14-4(b)(8).

30. What are other public relations and/or marketing considerations to be noted?

a. [No Response]

Evaluation Methodology

Objective 1: Indian Department of Environmental Management conduct modifications to Safe Drinking Water Information System to collect cybersecurity contact information for Indiana water and wastewater organizations by November 2017.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indian Department of Environmental Management maintains a cybersecurity contact information for 95 percent of Indiana water organizations serving a population greater than 3,301 by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis – Year 2
☒ Quantifiable Measurement
☐ Other

Deliverable: Cyber Risk Model (Plan)

Deliverable: Cyber Risk Model (Plan)

General Information

1. **What is the deliverable?**
    a. The deliverable is a risk framework assessment tool for the industrial control system that uses the NIST Cybersecurity Framework and AWWA Cybersecurity tool that is end-user friendly. The tool should have the capability to be completed through a one-day onsite visit. The resulting tool could be modified by other working groups and organizations to fit specific needs that may not be found in the water/wastewater industrial control systems.

2. **What is the status of this deliverable?**
    a. The risk framework has been established as a draft document. The effort has been put on hold while the cybersecurity risk template is prepared for SEA 362.

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☒ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The result will be a standard method for organizations to perform a risk assessment that is user friendly and the capability to conduct onsite visits. Currently, organizations are using various methods and standards to perform assessments. This deliverable will be consistent with the NIST framework and industry-specific AWWA cybersecurity tools.

6. **What metric or measurement will be used to define success?**
    a. Testing will be performed by conducting two risk assessments (RA) on Indiana water companies. Success will be the refinement of the templated assessment to enable completion of an assessment within a day for organizations with varying business structures and size.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Water and wastewater entities will benefit by having a mitigation report and areas of improvement identified. Entities will be able to demonstrate improvement by using a consistent tool for measuring improvements to their cyber posture. Other entities with industrial control systems will benefit by using the template tailored specifically to their organizations.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Department of Homeland Security has an assessment through the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) that provides similar results.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. We believe other groups with similar initiatives could share the product outcome for performing their own assessments within their groups.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Finance Authority (IFA) to provide resources in order for entities to complete assessments.
    b. American Water Works Association has expressed an interest in Indiana's initiatives focusing on cybersecurity for the industry.
    c. Academia (IUPUI / Purdue University) in the development of the assessment and resources to perform assessments.
    d. DHS ICS-CERT would be beneficial to come alongside the working group to share resources and development tools.

12. Who should be main lead of this deliverable?

a. Professor Connie Justice

13. What are the expected challenges to completing this deliverable?

a. Challenges are the resources to develop the assessment template. Once developed additional resources to perform the assessments: 500 + entities * 8 hours = 4,000 contact hours.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Questionnaire	Justice / Water and Wastewater Group	100	April 2018	
Risk Assessment Documentation	Justice	100	April 2018	
Risk Assessment Onsite Beta Test	Justice	100	April 2018	Risk Assessment Scheduled in April 2018 with Lewisville, IN Water. Risk Assessment scheduled with Speedway, IN Waste Water in April 2018.
Risk Assessment Report	Justice	0	September 2018	
Review Assessment Results with the Water and Wastewater Group	Water and Wastewater Group	0	October 2018	
Rewrite Questionnaire/Report if needed	Water and Wastewater Group	0	December 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following:**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
[N/A]					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Water and Wastewater Council Group	Expertise	0	0	N/A	N/A	
Graduate Students	Professional Education	0	0	N/A	N/A	
Dr. Justice	Expertise	0	0	N/A	N/A	
Dr. Kevin Morley, AWWA	Expertise	0	0	N/A	N/A	
Lewisville Water	Expertise	0	0	N/A	N/A	
Speedway Waste Water	Expertise	0	0	N/A	N/A	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The State of Indiana and AWWA risk assessment model for water and wastewater utilities. Allows a state-wide standard and measurement to assist each individual water and wastewater utility with measuring their risks and the State with calculating of state-wide risks.

b. Regularly conducted risk assessments close cybersecurity vulnerabilities and mitigate before the vulnerabilities are compromised. Therefore, allowing the sector to understand their cybersecurity posture.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Along with the action plan for each utility, the risk model will allow the water and wastewater companies to reduce the risk for their utility and will thus reduce risk to the State of Indiana overall.

b. The risk assessments allow for determination of a baseline security measure that can show improvement with additional risk assessment results. More importantly, the risk assessment will identify chinks in the armor of employee security education, training, and awareness (SETA). This will allow a proper SETA program to be initiated and maintained. Additionally, the risk assessment allows for the sector to prioritize the most sensitive areas of cybersecurity that need attention and investment.
c. We are unable to estimate the costs at this time but will be in a better position after utilities have completed risk assessments.

19. What is the risk or cost of not completing this deliverable?

a. If water and wastewater infrastructure is not protected, there could be a serious threat to the safety of the water supply and wastewater could breach into homes of Indiana citizens. Executive Order 13636 - Improving Critical Infrastructure Cybersecurity states that "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The baseline is an initial risk assessment score with mitigations to be implemented. Success is defined as successful completion of risk assessment with a score and the implementation of at least one mitigation recommendation.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. The AWWA has developed a cyber self-assessment tool that is available to any company nationwide that can be used by any water/wastewater utility. The AWWA has expressed interest in the Indiana cyber model tool that can be used across the country and will provide funding up to $40,000. We will describe the tool in our second deliverable

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The lack of volunteers' time to accomplish initial tasks.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. Water/Wastewater cybersecurity committee will work with the AIM committee, IDEM, and the IFA to ensure the template meets their requirements; and approved by IDEM and IFA as acceptable in order to meet State Law SEA 362

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. To support this deliverable in the future, a tool will need to be created to simplify the risk assessment for the sector client.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. AWWA, IDEM, AIM-Rhonda Cook, Stephanie Yeager; Chetrice Mosley, Dewand Neely, and Brian Langley.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. This risk assessment can be used by all sectors

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Indiana water and wastewater companies, AWWA, IOT, IDHS, IDEM

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Defer to Chetrice Mosley

Evaluation Methodology

Objective 1: IECC Water & Wastewater Committee and partners develop Cyber Plan Template for Indiana water/wastewater companies by December 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Water & Wastewater Committee and partners distribute Cyber Plan Template to twenty-five percent of Indiana water/wastewater companies by March 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Risk Tool

Deliverable: Risk Tool

General Information

1. **What is the deliverable?**
    a. The deliverable is a risk framework assessment tool for the industrial control system that uses the NIST Cybersecurity Framework and AWWA Cybersecurity tool that is end-user friendly. The tool should have the capability to be completed through a one-day onsite visit. The resulting tool could be modified by other working groups and organizations to fit specific needs that may not be found in the water/wastewater industrial control systems.

2. **What is the status of this deliverable?**
    a. Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☒ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The result will be a standard method for organizations to perform a risk assessment that is user friendly and the capability to conduct onsite visits. Currently organizations are using various methods and standards to perform assessments. This deliverable will be consistent with the NIST framework and industry specific AWWA (American Water Works Association) cybersecurity tools.

6. **What metric or measurement will be used to define success?**
    a. Testing will be performed by conducting 2 risk assessments on Indiana water companies. Success will be the refinement of the template assessment to enable completion of an assessment within a day for organizations with varying business structures and size.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Water and wastewater entities will benefit by having a mitigation report and areas of improvement identified. Entities will be able to demonstrate improvement by using a consistent tool for measuring improvements to their cyber posture. Other entities with industrial control systems will benefit by using the template tailored specific to their organizations.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Department of Homeland Security has an assessment through ICS-CERT that provides similar results.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. We believe other groups with similar initiatives could share the product outcome for performing their own assessments within their groups.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Finance Authority to provide resources in order for entities to complete assessments.
    b. American Water Works Association has expressed an interest in Indiana's initiatives focusing on cybersecurity for the industry.
    c. Academia (IUPUI / Purdue University) in the development of the assessment and resources to perform assessments.
    d. DHS ICS-CERT would be beneficial to come alongside the working group to share resources and development tools.

12. **Who should be main lead of this deliverable?**
    a. Professor Connie Justice

13. **What are the expected challenges to completing this deliverable?**
    a. Challenges are the resources to develop the assessment template. Once developed, additional resources to perform the assessments (500 + entities * 8 hours = 4000 contact hours).

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review and modify initial documents for accuracy	TBD	0	TBD based on funding	
Review with IOT to establish technical standards	TBD		TBD based on funding	
Establish detailed project plan	TBD		TBD based on funding	
Questionnaire	C. Justice/Water and Wastewater Group	0	TBD on project plan	NIST CSF/AWWA
Review Questionnaire	Water and Wastewater Group	0	TBD on project plan	
Risk Assessment Scoring Matrix	C. Justice	0	TBD on project plan	
Review of Risk Assessment Scoring Matrix	Water and Wastewater Group	0	TBD on project plan	Output score and where entity ranks in relation to others. Mitigation recommendations. Training needed
Risk Assessment Program Created	C. Justice /Programming Staff	0	TBD on project plan	Computer, tablet, mobile devices
Test Risk Assessment Program	C. Justice /Programming Staff	0	TBD on project plan	
Conduct Risk Assessment Sector	C. Justice/Water and Wastewater Group	0	TBD on project plan	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
[N/A]					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Dr. Justice	Risk Assessment Content	0	0		N/A	
Programmers	Programming expertise	80,000.00	TBD	State/AWWA	N/A	
IoT	Expertise	0	TBD		N/A	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Speed consistency, ease of use, the ability of water/waste water companies to conduct without third party support.
b. The ability to automate the risk assessment will allow for ease of use and automation of risk assessment results and the uploading of the data to a repository where the data can be referenced and used for baseline data for company and Indiana can use the data for measuring the effectiveness of the program.

18. How will this deliverable reduce the cybersecurity risk or impact?

a. More utilization since local water or wastewater utilities can use the tool to establish the utilities cyber risk profile.

19. What is the estimated costs associated with that risk reduction?

a. Estimated costs associated = 400 water companies x 16 hours x 2 people to conduct assessment onsite. Having an electronic tool will allow many, if not all, of the utilities to prepare the risk assessment themselves, thus reducing the estimated hours to conduct a manual risk assessment.

20. What is the risk or cost of not completing this deliverable?

a. If water and wastewater infrastructure is not protected, there could be a serious threat to the safety of the water supply and wastewater could breach into homes of Indiana citizens. Executive Order 13636 - Improving Critical Infrastructure Cybersecurity states that "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."

21. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. 80% will have conducted the assessment within 24 months of tool deployment.

22. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

23. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

24. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Program scope creep.
b. Problems with programming features of risk assessment software.

25. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

26. What will it take to support this deliverable if it requires ongoing sustainability?

a. Support of modifying model to changes of NIST model
b. IOT support to modify the tool

27. Who has the committee/working group contacted regarding implementing this deliverable?

a. IDEM, Chetrice Mosley, Dewand Neely, and Brian Langley

28. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. This risk assessment can be used by all sectors

Communications

---

29. Once completed, which stakeholders need to be informed about the deliverable?

a. Indiana water and wastewater companies, AWWA, IOT, IDHS, IDEM

30. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

31. What are other public relations and/or marketing considerations to be noted?

a. Defer to Chetrice Mosley

Evaluation Methodology

Objective 1: Water/Wastewater Committee develops Cyber Assessment Risk Tool within 12 months of securing funding.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Eight percent of Indiana water and wastewater companies will have used cyber assessment risk tool within 24 months of deployment.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Training Plan

Deliverable: Training Plan

General Information

1. **What is the deliverable?**
    a. The main deliverable is a Training Plan, consisting of three main components:
        i. An assessment survey that identifies the skills required by each actor within the system to fulfill their responsibilities utilizing the best practices of cybersecurity. Each skill will be mapped to a requirement for the industry, in the case of the Water Sector, the AWWA interpretation of the NIST standards. The skills themselves will be mapped against sources where the training required to satisfy the requirement can be obtained. A weighting will be assigned to each role/skill providing a scorecard of the skills gap.
        ii. A method for the reporting of assessment results into a (State) database to allow for the guidance of academia and course providers in the development and refinement of coursework, i.e., a managed database of training statistics.
        iii. A glossary of common terms will be developed to allow for cross sector utilization of the training plan. This will allow an organization to view cybersecurity holistically across their organization.

2. **What is the status of this deliverable?**
    a. Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

☒ Establish an effective governing structure and strategic direction.

☐ Formalize strategic cybersecurity partnerships across the public and private sectors.

☐ Strengthen best practices to protect information technology infrastructure.

☐ Build and maintain robust statewide cyber-incident response capabilities.

☐ Establish processes, technology, and facilities to improve cybersecurity statewide.

☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.

☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☒ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. The desired outcome of the Training Plan will be a significant reduction in the skills gap within Industrial Control System providers, Water Facility OT/IT personnel and associated admin and support staff.

6. **What metric or measurement will be used to define success?**
   a. The Training Plan will have as a central aspect a skills/responsibilities matrix with which an organization can map skills required by role and the training required to satisfy that requirement. Using the initial assessment as their baseline, they will able to quantify both their absolute gap and their growth, or lack thereof over each period.

7. **What year will the deliverable be completed?**
   a. 2019

8. **Who or what entities will benefit from the deliverable?**
   a. The completed and executed training plan will benefit each water entity that utilizes it to quantify their skills gap and then measure growth in developing critical cybersecurity skills in a prioritized manner.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. TBD

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. This is to be established. I will work with Ms. Mosley to define other sectors and/or committees that might have an interest in collaborating on this effort.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. TBD

12. Who should be main lead of this deliverable?

a. Cliff Campbell

13. What are the expected challenges to completing this deliverable?

a. Time and resources. This will require a significant effort in research and implementation.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop project plan	Training Working Group/Water and Wastewater Committee	0	TBD based on funding	
Develop roles by job function	Training Working Group/Water and Wastewater Committee			
Develop framework of skills required of each role within entity	Training Working Group/Water and Wastewater Committee	0	TBD on project plan	
Map skills to appropriate Standard	Training Working Group/Water and Wastewater Committee	0		
Cross reference skills to available training	Training Working Group/Water and Wastewater Committee	0		
Develop skills assessment scoring matrix	Training Working Group/Water and Wastewater Committee	0	TBD on project plan	
Skills Assessment Tool Created	Training Working Group/Water and Wastewater Committee	0	TBD on project plan	Computer, tablet, mobile devices
Validate Skill Assessment Tool	Training Working Group/Water and Wastewater Committee	0	TBD on project plan	

Coordinate with industry associations for distribution and collection of survey	Training Working Group/Water and Wastewater Committee	0	TBD on project plan	
Determine proper authority to host statewide database of skills	Training Working Group/Water and Wastewater Committee			
Determine relevant parameters to include in database	Training Working Group/Water and Wastewater Committee			
Create Database	Training Working Group/Water and Wastewater Committee			
Coordinate cross sector team to develop common glossary	Training Working Group/Water and Wastewater Committee			
Develop Common Glossary	Training Working Group/Water and Wastewater Committee			

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The State of Indiana and AWWA skills assessment model for water and wastewater utilities. Allows a state-wide standard and measurement to assist each individual water and wastewater utility with measuring their skills gap and the state with measurement of state-wide training needs.
b. Regularly conducted skills assessments close cybersecurity training gaps and mitigate before the vulnerabilities are compromised. Therefore, allowing the sector to understand their cybersecurity skills gap.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Along with an action plan for each utility, the risk model will allow the water and wastewater companies to reduce the risk for their utility and will thus reduce risk to the State of Indiana overall.
b. The skills assessments allow for determination of a baseline security measure that can show improvement with additional risk assessment results. More important, the risk assessment will identify chinks in the armor of employee security education, training, and awareness (SETA) so that a proper SETA program can be initiated and maintained. Additionally, the risk assessment allows the water/wastewater sector to prioritize the most sensitive areas of cybersecurity that need attention and investment.

19. What is the risk or cost of not completing this deliverable?

a. Along with an action plan for each utility, the risk model will allow the water and wastewater companies to reduce the risk for their utility and will thus reduce risk to the State of Indiana overall.
b. The risk assessments allow for determination of a baseline security measure that can show improvement with additional risk assessment results. More important, the risk assessment will identify chinks in the armor of employee security education, training, and awareness (SETA) so that a proper SETA program can be initiated and maintained. Additionally, the risk assessment allows the sector to prioritize the most sensitive areas of cybersecurity that need attention and investment.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Using the initial assessment as their baseline, they will able to quantify both their absolute gap and their growth, or lack thereof over each period. At a higher level, success can be evaluated on both a utilization percentage, as well as qualitative
b. The baseline is an initial risk assessment score with mitigations to be implemented. Success is defined as successful completion of risk assessment with a score and the implementation of at least one mitigation recommendation.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The lack of volunteers' time to accomplish initial tasks.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes
   i. Water/Wastewater cybersecurity committee will work with the AIM committee, IDEM, and the IFA to ensure the template meets their requirements; and approved by IDEM and IFA as acceptable in order to meet State Law SEA 362

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. [No Response]

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. [No Response]

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. This risk assessment can be used by all sectors

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Indiana water and wastewater companies, AWWA, IOT, IDHS, IDEM

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. [No Response]

Evaluation Methodology

Objective 1: Water/Wastewater Committee develop a training plan within three months of securing funding.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Fifty percent of Indiana water and wastewater companies incorporate the training plan as a part of their operational resources within 24 months of deployment of the training plan.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Cyber Plan Template

Deliverable: Cyber Plan Template

General Information

1. **What is the deliverable?**
    a. With the passage of SEA 362, water and wastewater utilities are required to have a cybersecurity plan. There is not an industry standard for cybersecurity plans for water or wastewater utilities. The NIST framework has the necessary items to establish one, but the framework is large and confusing for most water and wastewater utility personnel. There is a need for a simple and straightforward cybersecurity plan template that can be used to assist utilities in the establishment of their specific plan in order to comply with SEA 362.

2. **What is the status of this deliverable?**
    a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☒ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. What is the resulting action or modified behavior of this deliverable?

a. The result will be a standard method for utilities to establish and maintain a cybersecurity plan and program. This will provide for a significantly safer water delivery system for the State of Indiana.

b. The template is in development at this time. This draft template is currently "Open for Comments". It will continue this status for the next 60+ days. The current draft version of the template is contained in this plan's Supporting Documentation.

6. What metric or measurement will be used to define success?

a. Validation by the water and wastewater committee, with an approval vote. Review and certification of IDHS, IDE, IFS, and IOT.

7. What year will the deliverable be completed?

a. 2018

8. Who or what entities will benefit from the deliverable?

a. Water and wastewater utilities and the citizens of Indiana.

9. Which state or federal resources or programs overlap with this deliverable?

a. [No Response]

Additional Questions

10. What other committees and/or working groups will your team be working with to complete or plan this deliverable?

a. Local government.

11. Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?

a. Indiana Finance Authority will need to certify the plan template.

b. Indiana Department of Environment Management will need to certify the plan template.

12. Who should be main lead of this deliverable?

a. John Lucas, Chair of the Water/Wastewater committee

13. What are the expected challenges to completing this deliverable?

a. Getting the needed reviews in order to get the cybersecurity plan template completed.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Cyber Security Plan Template	Justice/Water and Wastewater Group	100%	October 2018	
Review of cyber security plan template by IDEM, IFS, AIM, and external partners	John Lucas	25%	December 2018	
Finalized cyber security plan template for distribution by IDEM.	IDEM, IFS, IDHS, Water and Wastewater committee	0	April 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
[N/A]					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Water and Wastewater Council Group	Expertise	0	0	N/A	N/A	
IDEM	Professional Education	0	0	N/A	N/A	
IFS	Expertise	0	0	N/A	N/A	
IDHS	Expertise	0	0	N/A	N/A	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. This will be the standard for all water/wastewater companies to establish a cybersecurity plan, and improve the cybersecurity of the water and wastewater utilities for the residents of the State of Indiana.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This will establish a baseline level of cybersecurity for all Indiana water & wastewater utilities. This plan will improve the utilities to protect utility assets and respond to a cyberattack much more quickly. This will reduce the risk to the residents of the state, and reduce the impact of an attack.

19. What is the risk or cost of not completing this deliverable?

a. Water and Wastewater utilities will not have a baseline for establishing a security posture, and will be unable to meet the requirements of SEA 362.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Establishment of a cybersecurity plan template, and the usage of this template to better secure water and wastewater utilities in Indiana.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No
b. **If Yes, please list states/jurisdictions**

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The short timeframe of this effort will put stress on the individuals who are writing the plan, and on the agencies who will be responsible for reviewing and implementing the plan.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes
    i. The water/wastewater cybersecurity committee will work with the AIM committee, IDEM, and the IFA to ensure the template meets their requirements; and approved by IDEM and IFA as acceptable in order to meet State Law SEA 362.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. This template will need to be updated regularly as cybersecurity standards and methods like the NIST standard change.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. IDEM, AIM-Rhonda Cook, Stephanie Yeager; Chetrice Mosley, Dewand Neely, and Brian Langley, IFS

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. This template could be used with modifications by other sectors.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Indiana water and waste water companies, AWWA, IoT, IDHS, IDEM, IFS

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. [No Response]

Evaluation Methodology

Objective 1: IECC Water and Wastewater Committee develop a Cyber Plan Template for Indiana water/wastewater companies by April 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Water & Wastewater Committee and partners distribute Cyber Plan Template to 50 percent of Indiana water/wastewater companies by October 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- IECC DRAFT Water and Wastewater Cybersecurity Plan Template

IECC Water and Wastewater Committee

Cybersecurity Plan Template

September 2018

DRAFT

WATER AND WASTEWATER CYBERSECURITY PLAN TEMPLATE

i. VERSION HISTORY

Date	Version	Description
05/29/2018	0.1	Initial Draft
6/7/2018	0.2	Modifications – Connie Justice
6/11/2018	0.3	Modifications- Sondhi Solutions
6/11/2018	0.4	Modifications – Connie Justice
6/17/2018	0.5	Modifications- Sondhi Solutions
06/20/2018	1.0	Second Draft – Connie Justice
6/21/2018	1.1	Modifications – Connie Justice and John Lucas
6/29/2018	2.0	Third Draft – Connie Justice
7/10/2018	2.1	Modifications-Connie Justice
7/20/2018	2.2	Modifications-Connie Justice
7/30/2018	2.3	Modifications – Connie Justice
8/15/2018	2.4	Modifications – Connie Justice
8/26/2018	3.0	Fourth Draft – Connie Justice
9/6/2018	3.1	Modifications – Connie Justice, John Lucas, Steve Berube, Jaimie Foreman, Jon Weirick

DRAFT

ii. Contributors and Acknowledgements

This cyber security template was developed by the Water / Wastewater committee of the Indiana Executive Cyber Security Committee of the State of Indiana. This committee is a committee of business, government, and regulatory members from across the State of Indiana.

iii. Important Terms

Term	Definition

DRAFT

iv. Table of Contents

i. Version History 2

ii. Contributors and Acknowledgements 3

iii. Important Terms 3

iv. Table of Contents 4

Introduction 1

Acronym List 1

Cybersecurity Plan Checklist 2

1 Identify 2

Return to Checklist 3

2 Protect 4

Return to Checklist 5

3 Detect 5

Return to Checklist 6

4 Respond 7

Return to Checklist 8

5 Recover 8

Return to Checklist 9

Exhibit 1: Data Classification Template 10

6 Exhibit 2: Critical Asset Inventory Per Facility 11

7 Exhibit 3: Policy Examples 12

8 Exhibit 4: Water Waste Water Risk Assessment (To Be Delivered) 13

9 Exhibit 5: Employee Training and Awareness 14

10 Exhibit 6: Securing Network and Cloud 15

11 Exhibit 7: Maintenance Life Cycle Process 17

12 Exhibit 8: Emergency Response Plan (ERP) 18

13 Exhibit 9: Contact List 19

14 Exhibit 10: After Action Report 20

DRAFT

INTRODUCTION

This document is a checklist of recommendations for maintaining the overall Cybersecurity posture of a Water or Wastewater Treatment operation. To be effective, each entity must ensure the cooperation of its IT Department, the Water and Wastewater Operations, and a Cybersecurity partner (if additional expertise in this area is required). Having a plan is only the first step. At least twice a year, you should verify that people, systems and software continue to align with your cybersecurity plan. Create a ledger to ensure you've covered identified recommendations. The guide is based on NIST cyber security framework and the EPA Incident Action Checklist – Cybersecurity. This document has been established in order for Water utilities to become compliant with Indiana Senate bill 362.

HOW TO USE THIS GUIDE

The document should be followed in the creation of policies, processes, and programs and verified by a Cybersecurity lead and clearly documented as part of the regularly executed Cybersecurity maintenance routine. A secure document management repository should be used to maintain and publish all documentation revisions.

DRAFT

ACRONYM LIST

IT	Information Technology
EPA	Environmental Protection Agency
NIST	National Institute of Standards and Technology
CSF	Cybersecurity Framework
AWWA	American Water Works Association
US-CERT	US-Computer Emergency Readiness Team
FFIEC	Federal Financial Institutions Examination Council
IDS	Intrusion detection system
TCP/IP	Transmission Control Protocol/Internet Protocol,
ICS	Industrial controls system
NIST SP	NIST Special Publication
ERP	Emergency response plan
NCCIC	National Cybersecurity & Communications Integration Center
INWARN	
IDHS	Indiana Department of Homeland Security
ISAC	Water Information Sharing and Analysis Center (WaterISAC)
WATER-ISAC	Water Information Sharing and Analysis Center (WaterISAC)

AAR	After action report
IP	Improvement plan
SOX	Sarbanes Oxley
HR	Human resources
PII	Personally identifiable information
HIPAA	The Health Insurance Portability and Accountability Act
SCADA	Supervisory control and data acquisition
CSRC	Computer Security Resource Center (CSRC)
SANS	SANS Institute was established in 1989 as a cooperative research and education organization
DMZ	Demilitarized zone
NMS	Network monitoring system
IPSEC	Internet Protocol Security
AES	Advanced Encryption Standard
WPA2	Wi-Fi Protected Access II
DHS	Department of Homeland Security
POC	Point of Contact

Cybersecurity Plan Checklist

Identify

- ☐ Identify Organization Security Lead
- ☐ Classify data
- ☐ Identify assets
- ☐ Security policies
- ☐ Risk Assessment
- ☐ Risk Management Strategy

Protect

- ☐ Employee Training and Awareness
- ☐ Access Control
- ☐ Securing Network and Cloud
- ☐ Authentication Policy
- ☐ Data Security
- ☐ Information Protection
- ☐ Maintenance
- ☐ Protective Technology
- ☐ Physical Access

Detect

- ☐ Anomalies and Events
- ☐ Continuous Monitoring
- ☐ Detection Processes

Respond

- ☐ Response Planning
- ☐ Respond Communications
- ☐ Analysis
- ☐ Mitigation
- ☐ Respond Improvements

Recover

- ☐ Recovery Planning
- ☐ Recovery Improvements
- ☐ Recovery Communications

DRAFT

1 IDENTIFY

When they happen, cybersecurity events are very stressful. This is not a time when you want to guess about who to call or where to find a serial number for an affected device. To help prepare for an event, it is important to create and maintain inventories of your assets. Knowing how those assets connect and work together is also very important. Having a list of contacts will ensure you have access to people and organizations in the event of an emergency. Building and maintaining an Information Technology Asset Inventory ensures you have critical information on your organization's technology items as they come in and out of their life cycle. Give each asset a unique code and label when entered into the inventory as they come into operation. Review the inventory at least annually and note items that are nearing "end of life" and plan to retire or replace them. Appendix A: IT Asset Inventory has a template to help you get started.

1.1 ORGANIZATION SECURITY LEAD

a. Identify an organization security lead
b. Identify emergency response team

1.2 ASSET MANAGEMENT

a. Identify mission critical data assets and classify data assets in order of importance. Identify personnel responsible for data asset/s.
b. See Exhibit 1 for data classification template
c. Identify mission critical assets
    a. Identify Mission Critical Technology Assets
        1. Applications (email applications, web browsers, productivity applications)
        2. Data (What storage devices data is stored on: hard drives, portable media, off site data backups)
        3. Servers (hardware devices that can host applications, or other virtual servers)
        4. Workstations/HMI/PLC (Systems that run SCADA software, Systems that run Business Software)
        5. Field devices (Laptops, Tablets, Cell Phones)
        6. Communications and network equipment (router, firewall, voice system)

Note: See Exhibit 2 for asset identification table template.

1.3 BUSINESS ENVIRONMENT AND GOVERNANCE

a. Governance framework is used to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.
b. Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.
c. Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.
d. Security Policies and Procedures Exhibit 3

DRAFT

1.4 Risk Assessment

1.4.1 Conduct a Risk Assessment

a. Execute a cybersecurity risk assessment to identify vulnerabilities in business and industrial control mission critical systems using the NIST CSF/AWWA tool (Link to Indiana Water/Wastewater Risk Model will be added).
b. Create action plan to mitigate significant vulnerabilities identified in risk assessment, and act on the mitigation plan.
    a. Create an action plan that prioritizes actions needed to mitigate risk.
    b. Prioritize the implementation of protective measures
    c. Low hanging fruit-Optimize your budget in relation to identified risks.

1.4.2 Risk Management Strategy

a. A security program established to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks.
b. Risk management is the process of identifying what information requires what level of protection and then implementing the proper level of protection and subsequently monitoring the protection.
The basic risk strategy is:
    a. Identify basic information stored and used in the business
    b. Determine the classification or value of the information
    c. Inventory the assets in the business
c. Understand what threats and vulnerabilities exists in the business

DRAFT

1.5 *Links for IDENTIFY Section*

a. US-CERT's Protect Your Workplace Posters & Brochure: http://www.us-cert.gov/reading_room/distributable.html
b. Socializing Securely: Using Social Networking Services: http://www.us-cert.gov/reading_room/safe_social_networking.pdf
c. Governing for Enterprise Security: http://www.cert.org/governance/
d. FFIEC Handbook Definition of Reputation Risk: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk- management/reputation-risk.aspx
e. What Businesses can do to help with cyber security: http://www.staysafeonline.org/sites/default/files/resource_documents/What%20Businesses%20Can%20Do%202011%20Final_0.pdf

Return to Checklist

2 PROTECT

The next step in your cybersecurity plan should be to determine what protections to put in place. This helps to limit exposure and limit damage in the event of an attack. Protections can include the following:

a. A way to control access to the IT assets you identified in Step 1.
b. A plan to provide cybersecurity awareness and training to your staff
c. A method to determine how to keep data, networks and systems secure
d. A plan to make sure systems are up-to-date with patches or if you can't patch systems then have appropriate controls to make sure systems are not modified (i.e. Scada systems with whitelisting).
e. A decision to use protective technologies to help prevent threats if appropriate

2.1 EMPLOYEE TRAINING AND AWARENESS

Employees should be trained and be aware of cybersecurity issues and situations that can compromise the business and ruin the company's reputation. See Exhibit 5 for training and awareness guidelines.

2.2 ACCESS CONTROL

2.2.1 SECURING NETWORK AND CLOUD

The network infrastructure is the backbone for defenses against internal and external malicious programs and nefarious persons. Layered protection and various devices are the key to protecting internal networks from these bad actors. Cloud services are becoming common place to conduct business. Ensure secure communications and multifactor authentication are setup between the business and cloud providers. See Exhibit 6 for example template of securing network and cloud.

DRAFT

2.2.2 IMPLEMENT A RIGOROUS USER AUTHENTICATION POLICY

a. Multifactor-authentication should be used wherever possible.
b. Use a passphrase instead of a password. A passphrase is a phrase constructed of multiple words. An example would be: "sunwalkraindrive". A passphrase constructed of 4 words (sun + walk + rain + drive) is easy to remember but hard to guess. It is not recommended that users change their passwords because of the general predictability in which users change specific characters.
c. Use unique passphrases for separate confidential accounts.

2.2.3 DATA SECURITY

In addition to understanding data classification, it is important to protect business data. Sensitive business data should be encrypted on storage medium and data should be encrypted in transit from end to end communications. The key elements to secure data are:

a. Data at rest is encrypted
b. Data in transit is encrypted
c. Logging in place to protect against data leaks
d. Systems in place to ensure integrity of data

2.3 Information Protection Processes and Procedures

Data should also be protected by proper backups and testing. Additionally, proper destruction of data is very important, as well as having an incident response, disaster recovery, and business continuity plan in place.

a. Backup and restore of data are tested
b. Data destruction process is in place
c. Incident response, disaster recovery, and business continuity plans are in place and managed.

2.4 Maintenance

Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity. See Exhibit 7 for the asset management process.

2.5 Protective Technology

a. Storage media management and disposal program established to ensure that any sensitive data/software is used appropriately and is removed prior to media disposal (including approved policies and procedures).
b. Centralized logging system including policies and procedures to collect, analyze and report to management.
c. SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.
d. Program for hardening servers, workstations, routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).

DRAFT

2.6 Physical Access

a. Physical access to facilities and areas where operational equipment is running should be limited to staff who require the access to perform their job. A more liberal policy on access control is not best practice and would inevitably provide access to individuals who accidently or purposefully create problems with the environment.
b. Physical Security should be implemented to ensure access is given to areas with operational or IT systems only to those personnel who need access to these areas to perform their job duties.
c. No access to the internet should be permitted to industrial control systems unless absolutely required. If required, a web content filter should be used to limit the access to the system based on a policy.

Return to Checklist

3 Detect

Organizations must implement the appropriate measures to quickly identify cybersecurity events. The adoption of continuous monitoring solutions that detect anomalous activity and other threats to operational continuity is required to comply with this function. Organizations should have network

visibility in order to anticipate a cyber incident; which should be included in your current cybersecurity plan.

3.1 Anomalies and Events

a. An intrusion detection system (IDS) should be implemented to identify malicious activity. IDS systems are designed to watch for signatures of malicious traffic, or to recognize anomalies in the underlying TCPIP communications. If anything falls outside of the normal patterns for how these protocols work, the IDS will send an alert to the administrator for the system who can then act upon the alert by implementing a firewall rule to block the offensive traffic.
b. Security Continuous Monitoring. A basic logging server should be deployed to aggregate log data from different devices to correlate alerts and notify the administrator when certain thresholds have been met (e.g. 3 or more failed logins for an account).

3.2 Security Continuous Monitoring

a. Monitoring for unauthorized personnel, connections, devices, and software is performed
b. Active monitoring for adversarial system penetration
c. Intrusion prevention systems should be configured to monitor for suspicious activity crossing your network perimeter
d. If you use a web filtering system, employees should have clear knowledge of how and why their web activities will be monitored, and what types of sites are deemed unacceptable by your policy.
e. Identification of security deficiencies in existing hardware and software.

DRAFT

3.3 Detection Processes

a. Continuous monitoring is a very effective way to analyze and prevent cyber incidents in ICS networks. Use intrusion detection systems, intrusion prevention systems and file integrity checkers to spot intrusions and verify web content.
b. Register for cybersecurity alerts and advisories from water sector and government partners to be aware of new vulnerabilities and threats (two sources of cybersecurity alerts are WaterISAC, which has a basic membership that is free, and ICS-CERT (https://ics-cert.us-cert.gov/alerts)).
c. Ensure the ICS network is separated from the public network. Additionally, the business network should be segmented from the ICS network using industry best practices (NIST SP 800-82 section 5).
d. Restrict internet access to industrial control systems unless there is a critical need.
e. System acceptance standards including data validation (input/output), message authenticity, and data integrity established to detect information corruption during processing.

Return to Checklist

4 Respond

a. Should a cyber incident occur, organizations must have the ability to contain the impact. To comply, your organization should utilize your response plan which should include processes such as:
    i. define communication lines among the appropriate parties
    ii. collect and analyze information about the event
    iii. perform required activities to eradicate the incident
    iv. incorporate lessons learned into revised response strategies.
b. The Emergency Response Plan (ERP) should be referenced and adhered to in the event of a Cybersecurity incident. The Emergency Response Team should be comprised of essential personnel that should be contacted, followed by the contacts listed in the Emergency Response Plan including all other utility personnel and media outlets as necessary. NCCIC can also assist with critical system response and recovery (888-282-0870 or NCCIC@hq.dhs.gov)

4.1 Response Planning

A security and response program should be established to ensure staff is aware of security policies and incident response/notification procedures. See Exhibit 8 for ERP steps.

DRAFT

4.2 Communications

Contacts

a. Have ready access to a list of primary and backup contacts for personnel or entities (vendors, government agencies, etc.) responsible for the operation and maintenance of each critical system.
b. Next, identify priority points of contact for reporting a cyber incident and requesting assistance with response and recovery. Include any state resources that may be available such as Indiana State Police, Indiana National Guard Cyber Division or mutual aid programs (INWARN), as well as the Indiana Department of Homeland Security to assist with an attack and any other contact information needed. Exhibit 9: Emergency Contacts has a template to help organize necessary contacts.

4.3 Analysis

a. Investigate notifications from detection systems
b. Understand incidents
c. Incidents are categorized appropriately per response plans
d. A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.

4.4 Mitigation

a. Contain incidents
b. Mitigate incidents
c. Newly identified vulnerabilities are mitigated or documented as accepted risks

4.5 Improvements

a. Incorporate lessons learned from response plans
b. Update response plans

4.6 Contacts

4.6.1 Assess the damage to utility systems and any disruption to operations.

A checklist should be created for use in the Emergency Response Plan to verify functionality for critical business services and their supporting infrastructure. Any affected services should be documented and relayed to the administrator of the Emergency Response Plan. The administrator of the Emergency Response Plan should also document any reports of suspicious communications before or during the incident. The documentation should include date and time that information was reported.

4.6.2 Forensics Image

a. A forensic image should be taken of the impacted systems and transferred to other secure media that is not connected to a network. If possible, the original systems that were affected should be disconnected from the network and not powered down or rebooted.
b. After containment and a forensic image has been captured and the original system has been taken off the network and preserved for evidence, restore the system function to a new system from the last known good backup before the infection occurred.
c. Never work on the original evidence when responding to a Cybersecurity incident. This will ensure the integrity of the original evidence.

DRAFT

4.6.3 Lessons Learned

a. A Lessons Learned session should be conducted after an incident has been resolved. Each problem, it's perceived cause, and what should have been done differently should be discussed.
a. Positive feedback should also be discussed to show what went right during the response.
b. Submit the incident to WaterISAC and Indiana AWWA. The online WaterISAC incident report form can be found at https://www.waterisac.org/report-incident or a call can be placed at 866-H2O-ISAC. Additionally, report incident to Indiana AWWA.

Return to Checklist

5 Recover

5.1 Recovery Planning

Policies and procedures for system instantiation/deployment should be established to ensure business continuity.

5.2 Improvements

Develop a lessons learned document and/or an after action report (AAR) to document utility response activities, successes, and areas for improvement. Create an improvement plan (IP) based on your AAR and use the IP to update your vulnerability assessment, ERP and contingency plans. See Exhibit 10 for an example AAR report.

5.3 Communications

a. Organizations must develop and implement effective activities to restore any capabilities or services that were impaired due to a cybersecurity event. Organizations must have a recovery plan in place, be able to coordinate restoration activities with external parties and incorporate lessons learned into updated recovery strategy. Defining a prioritized list of action points which can be used to undertake recovery activity is critical for a timely recovery.
b. The organizations recovery plan should address damage to reputation from data breaches, criminal organizations, inappropriate employee actions.
c. Mission critical processes should be documented in the Emergency Response Plan, and the appropriate sequence should be determined and communicated by the Emergency Response Plan administrator based on the systems that have been affected.
d. If required, the public and media outlets should be notified of the incident.

Return to Checklist

DRAFT

EXHIBIT 1: DATA CLASSIFICATION TEMPLATE

Example Data Classification Template

Data	Classification	Justification	Data Owner	Data User
Executive Business Material	Restricted Confidential	Intellectual Property		Executives & Assistants
Bank Accounts - Information	Confidential	SOX		Financial Reporting
Financial Reporting Data	Confidential/Public - phases	SOX		Financial Reporting
Building Information	Confidential	SOX		Financial Reporting
Legal Case Information	Sensitive	Intellectual Property		Legal
Leasing Information	Confidential / Restricted Confidential phases	Intellectual Property		Leasing
Security video	Sensitive	Intellectual Property		Security
Custom Application Code	Sensitive	Intellectual Property		Information Services
Audit Information	Restricted Confidential	Data from all areas		Audit Services
Tax Filings	Sensitive			Corporate Tax
HR	Sensitive	PII, Laws		HR
Benefits	Confidential	HIPAA / do not submit		HR

DRAFT

Definitive guide to data classification:

https://infosecpartners.com/wp-content/uploads/2017/02/The-Definitive-Guide-to-Data-Classification.pdf

6 Exhibit 2: Critical Asset Inventory Per Facility

Facility Name: _____

AssetID	Item	Description	Serial #	Service Date	Retirement Date	Original Value	Current Value	Custodian	Department

DRAFT

7 Exhibit 3: Policy Examples

Policy Name	Description
Security Policy	A document designed for staff that should include the security program requirements and require signoff for employees.
Emergency Response Plan	Procedures to follow in the event of a Cybersecurity breach.
Password Policy	Outlines the specific password requirements for the organization.
Acceptable Use Policy	Defines how the internet and email should be used to promote a responsible culture around Cybersecurity.

- Guide to Industrial Control Systems (ICS) Security
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- Guide for Cybersecurity Event Recovery
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf
- 21 Steps to Improve Cyber Security of SCADA Networks
  https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf
- Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems
  https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf
- 10 ways to develop cybersecurity policies and best practices
  https://www.zdnet.com/article/10-ways-to-develop-cybersecurity-policies-and-best-practices/
- SANS Information Security Policy Templates
  https://www.sans.org/security-resources/policies

DRAFT

8 Exhibit 4: Water Waste Water Risk Assessment (To Be Delivered)

DRAFT

9 Exhibit 5: Employee Training and Awareness

a. Implement a cybersecurity awareness program that includes:
    i. Social engineering
    ii. Sharing of personal information
    iii. Phishing
    1. Types of phishing attacks
    2. What can happen as a result of Phishing
    iv. Ransomware
    1. What to do in the event your system has been compromised by Ransomware
    v. Email Best Practices and what to watch for
    vi. Internet browsing acceptable use policy
    vii. Authentication (password policy, use of multi-factor authentication, and remote access where required).
b. Provide on-going cross training for critical systems and ICS staff that identifies current best practices and standards for ICS cybersecurity.
c. Provide basic network and radio communications training for ICS technicians.
d. Participate in water sector programs that facilitate cybersecurity knowledge transfer.
e. Identify appropriate certifications for internal and external staff. Include certification requirements in SLAs and contracts with external service providers.
f. Provide periodic security awareness training to employees that identifies risky behaviors and threats.
g. Promote information sharing within your organization.

DRAFT

10 Exhibit 6: Securing Network and Cloud

a. Network
   i. Network Separation
      1. Business systems such as email or other systems that require access to the internet should be managed on a separate physical network from the water/wastewater operation systems.
      2. A DMZ should be established for any traffic originating from outside of the internal network, although traffic of this origin should be eliminated where possible and ensure there is no connectivity to the Water/Wastewater systems network.
   ii. Network Hardware
      1. Have records of current hardware and software configurations.
      2. Maintain support contracts with critical software vendors, for example: endpoint protection (anti-virus, malware detection, log monitoring) and operating system patches in accordance with each vendor's recommended patch level if applicable
      3. It is important to maintain support contracts for software programs required to maintain the operation or protect/backup the systems.
         a. There could also be a delay in gaining access to critical software patches or system support if there is a lapse in support coverage.
         b. Software patches should be first tested on an offline system that doesn't have access to the Water/Wastewater Industrial Control System network.
         c. Once the patch is demonstrated to be safe, it can be scheduled on actual production systems.
   iii. Monitoring
      1. An NMS should be implemented to ensure alerts are sent to the network manager when a device is unavailable for a pre-determined period of time.
      2. System and Event Logs should be monitored for critical events that occur, and alerts sent to the network manager.
   iv. Cloud
      1. Interfacing with cloud environments
      2. IPSEC tunnels should be used between on premises networks and public cloud networks
      3. Firewalls should be used in cloud-based network for separation in the same manner recommended on internally hosted systems.
      4. Centralized authentication authority and multi-factor authentication should be used when accessing public cloud environments.
b. Server and Workstation Hardening:
   i. Disable services that are not required
      1. Use whitelisting software to only allow execution of required applications.
      2. Ensure system-based firewalls are not more permissive than they need to be – only allow what is absolutely necessary.
      3. Disable built-in, default accounts.
      4. Access Control should be employed and provide multi-factor authentication, pass phrases made up of 4 regular words, and unique passwords for different systems. Operational systems and Business systems should reside on two separate physical networks separated by firewall devices.
      5. Service Level Agreements (SLAs) should be included in vendor contracts to ensure they are providing the amount of internet bandwidth and round-trip speeds agreed

DRAFT

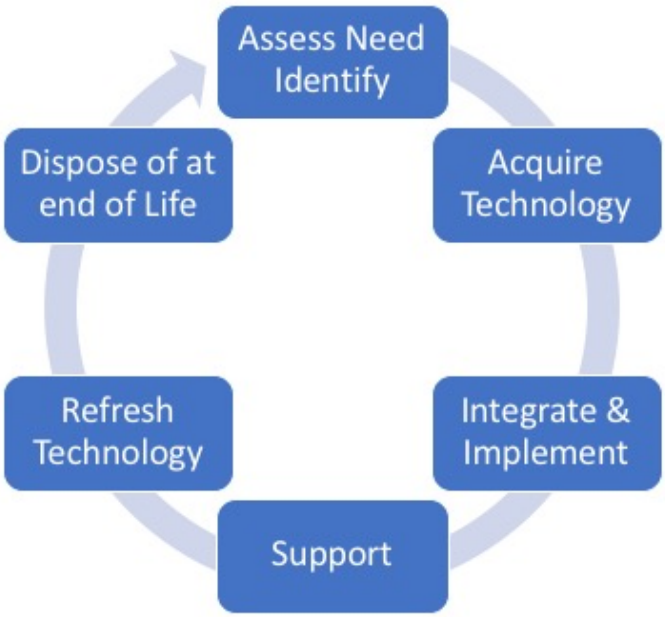
to in the contract, and that 3rd party personnel that work on utility systems are certified based on agreed upon industry standard certifications based on their job function.

c. Wireless and Wireless guest access secured by strong protocols, such as WPA2 with AES encryption.

DRAFT

11 Exhibit 7: Maintenance Life Cycle Process

Asset Lifecycle Management Process



12 Exhibit 8: Emergency Response Plan (ERP)

An emergency response plan (ERP) is important if a cybersecurity incident were to occur that requires notification outside of the primary business. The following is a guide for possible ERP action items:

1. Contact Law Enforcement-if required
2. Contact government authorities-if required
3. Notify customers
4. Record the data lost or exposed
5. Record measures taken to reduce future exposure
6. Technical and leadership work to limit damage
7. Containment
8. Reputation risk management
9. Request outside assistance if needed
10. Begin recovery
11. Eradicate malware
12. Hold lessons learned meeting
13. Discover knowledge gained during the incident
14. Document knowledge gained during the incident
15. Refine knowledge gained during the incident

DRAFT

13 Exhibit 9: Contact List

Contact Name	Organization Name	Phone	Email	Website
	Law Enforcement			
	IT Staff/Vendor			
	SCADA Staff/Vendor			
	DHS NCCIC	888-282-0870		
	Local Laboratory			
	State Primacy Agency			
	Local Emergency Management Agency			
	Local Health Department			
	IWARN Chair			
	State Emergency Management Agency			

DRAFT

14 Exhibit 10: After Action Report

Incident Name	[Insert the formal name of exercise, which should match the name in the document header]
Incident Dates	[Indicate the start and end dates of the incident]
Description	This incident …
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor)]

[Incident]

The strengths and areas for improvement for each core capability aligned to this objective are described in this section.

DRAFT

[Incident Description]

Strengths

The [full or partial] incident can be attributed to the following:

1: [Observation statement]

2: [Observation statement]

3: [Observation statement]

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: [Observation statement. This should clearly state the problem or gap; it should not include a recommendation or corrective action, as those will be documented in the Improvement Plan.]

Reference: [List any relevant plans, policies, procedures, regulations, or laws.]

Analysis: [Provide a root cause analysis or summary of why the full capability level was not achieved.]

Area for Improvement 2: [Observation statement]

Reference: [List any relevant plans, policies, procedures, regulations, or laws.]

Analysis: [Provide a root cause analysis or summary of why the full capability level was not achieved.]

DRAFT

APPENDIX D.10
WORKFORCE DEVELOPMENT COMMITTEE

WORKFORCE DEVELOPMENT COMMITTEE STRATEGY PLAN

Chair: Commissioner Fred Payne | Co-Chair: Dr. John Keller

September 2018
Indiana Executive Council on Cybersecurity

Workforce Development Committee Plan

Contents

Committee Members **4**

Introduction **6**

Executive Summary **8**

Research **10**

Deliverable: Generate Interest Plan **13**

General Information 13

Implementation Plan 15

Evaluation Methodology 21

Deliverable: Job Demand Tool **23**

General Information 23

Implementation Plan 25

Evaluation Methodology 29

Deliverable: K-12 Offering Cybersecurity Content **31**

General Information 31

Implementation Plan 33

Evaluation Methodology 39

Deliverable: NICE Framework Standard **41**

General Information 41

Implementation Plan 42

Evaluation Methodology 46

Deliverable: Incentivized Cybersecurity Certifications **49**

General Information 49

Implementation Plan 51

Evaluation Methodology 55

Deliverable: Program Data Tool **57**

General Information 57

Implementation Plan 59

Evaluation Methodology 63

Supporting Documentation **65**

National Governor's Association (NGA) Policy Academy Indiana 1st Workshop Notes 66

Committee Members

Committee Members

Name	Organization	Title	Committee Position	IECC Membership Type
Fred Payne	Indiana Department of Workforce Development	Commissioner	Chair	Voting
Jeff Tucker	Indiana Department of Workforce Development	Chief Information Officer	Chair Proxy	Voting Proxy
Dr John Keller	Indiana Department of Education	Chief Technology Officer	Co-chair	Advisory
Sean Roberts	Code.org	Director of State Government Affairs	Full Time	Advisory
David Greer	Project Lead The Way	Senior Vice President and Chief Program Officer	Full Time	Advisory
Benjamin Carter	Indianapolis Public Schools	Director of Career & Technical Education	Full Time	Advisory
Jim Goldman	Salesforce	VP, Security Governance, Risk Management & Compliance	Full Time	Advisory
Geanie Umberger, PhD	Purdue University	Associate Dean for Engagement	Full Time	Advisory
Nick Taylor	E-gineering	Owner	Full Time	Advisory
Shane Springer	Indiana Department of Workforce Development	Director of Government & Legislative Affairs	Full Time	Advisory
Matt Etchison	Ivy Tech	Vice President of Information Technology	Full Time	Advisory
Dan Calarco	Indiana University	Chief of Staff,	Full Time	Advisory
Doug Rapp	Cyber Leadership Alliance	President / CEO	Full Time	Advisory
Michael Hawryluk	Indiana Commission for Higher Education	Chief Technology Officer	Full Time	Advisory
Teresa Lubbers	Indiana Commission for Higher Education	Commissioner	As Needed	Voting
Jim Weber	Raytheon	Cyber Security and Specialty Engineering Department Manager	Full Time	Advisory
Matt Norris	Krieg DeVault LLP		Full Time	Advisory
Walt Grudzinski	Vectren Corporation	Director of Information Security and Business Continuity	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Searched for:
    - Valid and complete list of all cybersecurity courses/programs/degrees/etc
    - Source for current and future demand for cybersecurity workers in Indiana
    - List of all cybersecurity-related jobs and the skills required to fill those jobs
    - Info on how easy/difficult it is to fill cybersecurity jobs, currently
    - List of programs designed to generate interest in cybersecurity and a career in cybersecurity
    - What has happened in the recent past in this area in Indiana
    - Existing data on cybersecurity programs/courses/degrees/certifications and the capability of that data

- **Research Findings**
  - It is difficult in most cases to quickly fill cybersecurity-related jobs with people who have the required skills
  - International Economic Development Council (IEDC) Cyber Initiative report provided a starting point for many of our committee's desired deliverables – framework, program list, job demand challenges, etc.
  - The National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) has developed a Cybersecurity Workforce Framework. This framework provides a common language to be used to describe tasks, knowledge, skills, and abilities needed for each cybersecurity work role. This framework is being reviewed by other states and has been adopted by at least two states.
  - There are many existing and effective programs to generate interest in cybersecurity, measure aptitude, provide needed skills and/or certifications, etc. This committee's initial efforts on many of our deliverables will be to develop effective ways to leverage these existing initiatives before trying to create something new.
  - There are other closely related programs to which cybersecurity content could be added to further promote the field of cybersecurity and generate interest.
  - Existing data on cybersecurity programs/courses/degrees/certifications may not be granular enough to satisfy all of our committee goals. Needs further investigation.

- **Committee Deliverables**
  - Generate Interest Plan
  - Job Demand Tool
  - K-12 Offering Cyber Security Content
  - Best Practices and NICE Framework Standard
  - Incentivized Cybersecurity Certifications
  - Program Data Tool

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity**?
    a. Not Applicable

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Near-term challenge – a shortage of people with needed skills to fill open cybersecurity positions. The longer-term challenge will be the strategic filling of the pipeline to ensure Indiana is well positioned not just to fill open cybersecurity positions, but to also provide a workforce that would aid in attracting cybersecurity firms to locate in Indiana.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Biggest need is people with cybersecurity skills to fill open cybersecurity jobs.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Not Applicable

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. From a workforce perspective – there is a Cybersecurity Workforce Framework that has been developed by the National Initiative for Cybersecurity Education (NICE) which is a part of NIST. This framework provides a common language to be used to describe tasks, knowledge, skills, and abilities needed for each cybersecurity work role. This framework has begun to be adopted by other states and tools are being developed to facilitate the implementation of the framework (e.g, a job description writing tool).

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. Indiana has plenty of data about the current state of affairs at various levels of the cybersecurity pipeline including data from Indiana Department of Education (IDOE), Department of Workforce Development (DWD), and Commission for Higher Education (CHE). The IEDC Cyber Initiative report provided a starting point for many of our committee's desired deliverables – framework, program list, job demand challenges, etc.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. See answer to #5 above.
    b. Cybersecurity course being developed by Project Lead the Way for 10th graders.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Sufficient quantity of skilled workers to fill all cybersecurity positions. Ability to see current and future demand for all cybersecurity jobs. Ability to understand the skills associated with all jobs that make up the demand. Ability to see all students in the pipeline that are in programs that provide them the needed skills to fill that demand. A better alignment of activity in the K-12 system and the nurturing that needs to happen to progress from broad competencies in early grades to focused skills and proficiency as students move through high school and into college.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. This is what our committee is working on as part of the IECC.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. Due to limitations in how this data is gathered, an accurate number is difficult to determine. Anecdotal data suggests that there are not enough cybersecurity workers to fill all open positions. It is likely that in many cases, employers are filling these positions and providing or arranging for the appropriate training. A key deliverable for our team is to develop methods/models to identify the current and future demand for all cybersecurity jobs in Indiana – the types of cybersecurity jobs and the required skills. It is reasonably assumed that the need for cybersecurity-skilled workers will grow and one specific need will be for K-12 instructors – this may provide an opportunity to look into the feasibility of engaging individuals with cybersecurity expertise as instructors even though they don't have teaching licenses.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. The primary requirement from our Committee's perspective - provide a capable and skilled workforce.

12. **What are your communication protocols in a cyber emergency?**
    a. Not Applicable

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. National Initiative for Cybersecurity Education Cybersecurity Workforce Framework – provides a common language for all cybersecurity work roles and the tasks, knowledge, skills, and abilities needed for each.

Deliverable: Generate Interest Plan

Deliverable: Generate Interest Plan

General Information

1. **What is the deliverable?**
    a. Increase awareness and interest in cybersecurity careers and degree attainment
    b. Increase the number of Indiana high school graduates with an industry-recognized cybersecurity-related certification
    c. Incentivize and encourage participants to seek education, live and work in Indiana
    d. Provide a pipeline of students that are prepared to successfully achieve post-secondary career goals in cybersecurity.
    e. Utilizing the National Governors Association (NGA) Policy Academy work, develop a proposal to fund and sponsor the rollout of an initiative with the goal of creating a program centered on Cybersecurity, or sponsor a program the covers Pre-K through postsecondary. The Academy also identified the need to pilot professional development programs across the state to increase student interest, awareness, and efficacy in cybersecurity.
    f. Develop and support workforce development programs that provide:
        i. A robust technology platform that includes portals for primary to secondary teachers, instructors and students with career pathways, curricula, and project-based resources
        ii. Resources for teachers related to professional development
        iii. Assessment tools for companies, employees, government for assessing cybersecurity aptitudes and abilities of employees
        iv. Apprenticeship programs for preparing the cybersecurity workforce
        v. Co-ops and internships programs available across the state.
        vi. Middle/high school level network of cybersecurity camps, clubs, and competitions that can incorporate industry-recognized certification curriculum into classroom instruction, with opportunities for students to receive certifications upon completion.
        vii. Fund the curricula development for high school students to graduate with a certificate in cybersecurity, instructed by teachers who have received professional development in cybersecurity.
        viii. Create access and opportunity for underserved and underrepresented populations
    g. Examples include Cyber Patriot (listed in the following planning pages), IN CyberPath, and GEN Cyber.

2. **What is the status of this deliverable?**
    a. In-progress; 25% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   - ☐ Establish an effective governing structure and strategic direction.
   - ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   - ☐ Strengthen best practices to protect information technology infrastructure.
   - ☐ Build and maintain robust statewide cyber-incident response capabilities.
   - ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   - ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   - ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity**.**

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   - ☐ Research – Surveys, Datasets, Whitepapers, etc.
   - ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   - ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   - ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   - ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   - ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

---

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Per the NGA Academy, need to develop a system that instills cybersecurity understanding, education, and ethics throughout a student's entire journey, from Pre-K through post-career.
   b. Provides a mechanism to generate interest among grades Pre-K through 12th grade globally in computer science and specifically in Cybersecurity.
   c. Offers the opportunity for advanced students to graduate high school with a cybersecurity certification, qualifying them for entry-level cybersecurity jobs.

6. **What metric or measurement will be used to define success?**
   a. Number of programs state-wide
   b. Number of participants statewide in the program.
   c. Number of cyber camps state-wide
   d. Creation of statewide cyber competition

7. **What year will the deliverable be completed?**
   a. 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Students
    b. Universities (potentially broaden the pool of degree seekers in cybersecurity).
    c. Private and government sector job market
    d. Industries and general public (greater security for their private information)

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Programs such as these would probably be in line for funding for STEM (Science, Technology, Engineering, and Math) grants from either state, federal or philanthropic sources with missions aimed at increasing attainment in these areas.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Other high-level cybersecurity program developers. Cyber Patriot is one of a number of programs that could increase informal opportunities for middle and high school students.
    b. Indiana CyberPath program developed collaboratively between Purdue University (Career Makers) and Indiana University (Center for P-16 Research and Collaboration).
    c. A cybersecurity framework that can be adopted in other states.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Potentially the IDOE (state agency)
    b. Indiana Economic Development Corporation (IEDC)
    c. Lieutenant Governors (LG) Office
    d. The Cyber Leadership Alliance
    e. Any number of private organizations, industry professional and industry associations, and non-profits could have a funding interest in Cyber Patriot, Indiana CyberPath, or other similar programs.
    f. Other state universities as necessary to ensure a robust plan

12. **Who should be main lead of this deliverable?**
    a. The Cybersecurity program developers
    b. Appropriate state agencies (e.g. DWD, IDOE, IECC) provide implementation support from an organization with domain expertise and implementation know how.

13. **What are the expected challenges to completing this deliverable?**
    a. Funding
    b. Logistics
    c. Coordination with broader interest generating efforts
    d. Dissemination of the deliverables across the state

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable (two-year initiative)

Tactic Timeline – Sample Program: Cyber Patriot

Tactic	Owner	% Complete	Deadline	Notes
Prep & Plan	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	80%	Award of funding (A)+2	
Awareness (Marketing campaign)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+3	
Identify Schools	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	10%	A+4	There are 70 existing programs in Indiana
Club Sponsor /Faculty Training event	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+5	Regional
Camps yr. 1	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	40%	Jun18-Aug18	Venues and sponsors for camps identified
Training event (certification curriculum)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	Jun18-Aug18	
Club yr. 1	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	Aug18-May19	
Regional & State finals @ MUTC	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	20%	Jan19/Feb19	Commitment from the Indiana National Guard to host and sponsor
Camps yr. 2	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	40%	June19-Aug19	Venues and sponsors for camps identified

Club yr. 2	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	Aug19-Jun20	
Regional & State	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	Jan20/Feb20	
Identify corporate sponsors	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	50%	A+9	Cyber Leadership Alliance members have made tentative commitments
Refine established baseline metrics	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+11	Initial metrics
Grant winner training	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+17	Top performing clubs will receive small grant to offset cost of State competition & training
Competition/ Training event	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+18	
Program Review	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+24	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Line Item	Price	In Kind	Description
Marketing	$20,000.00		ad space, social media campaign, events
Collateral	$10,000.00		physical & virtual materials to support campaign
Messaging	$10,000.00		strategy & messaging of campaign
Training/Kick-off Event	$12,000.00		train-the-trainer event
Regional	$8,000.00		CLA to travel regionally and provide 4 hr seminar in 4 locations
Registration	$22,960.00		Cover cost of registration to incentivize participation. 5% Yr1 & 10% Y2
Supplies	$11,200.00		general supplies
Stipend	$44,800.00		Incentivize teacher participation
Equipment Grant	$10,000.00		free and reduced lunches, ensuring underserved communities meet technical requirements
Certification Grant	$15,000.00		25 grants to top 5% students based upon market penetration
Curriculum	$7,500.00		5 Camps, 1 week of pre-packaged CyberPatriot curriculum
Staff	$15,000.00		2 instructors, $1500 a week
F&OH	$7,000.00		5 locations, $1000 week to cover facility & lunch
Team Scholarship	$10,000.00		20 team scholarships @ $500/team to offset travel expenses
MUTC Facility & OH	$15,000.00		2 day in-person, cyber physical competition @ IN Nat'l Guard MUTC. F&OH, Range Access
Exercise Director	$125,000.00	$ (125,000.00)	Exercise director, all-inclusive cyber-exercise. Scenario & exercise design, red-team, on-site technical support
Coordinator	$35,000.00		50% of full-time implementation coordinator
Project MGMT & Leadership	$65,000.00		50% of full-time project manager/senior consultant
Subtotal	$443,460.00		
In Kind	$ (125,000.00)		
Grand Total	**$ 318,460.00**		

- Funding sources: Request funding from State of Indiana with a significant match from private industry.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. This initiative will educate, grow, and help to retain an Indiana based workforce by focusing on pre-K through 12th grade students, community college and university students, underrepresented and underserved populations, veterans, incumbent workers requiring re-training, minor offenders, and more.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. [No Response]

19. What is the risk or cost of not completing this deliverable?

a. According to the Indiana Department of Workforce Development (DWD), Indiana needs to fill more than one million jobs over the next decade. Of those million jobs, more than a third will be new or growth occupations within the state. As the nature of work continues to change at an accelerated pace, the workforce will need new skills to meet the challenge at all levels of education. It is estimated that nearly 30,000 job openings per year will require an industry-recognized certificate/certification in addition to a high school diploma. Without this initiative, Indiana will continue to leave approximately 2,500 cybersecurity jobs statewide unfilled creating an incalculable risk to industry, wealth, and citizenry.

b. Indiana students will continue to graduate from high school lacking the necessary background to successfully achieve cybersecurity career goals, much less an understanding of cyber hygiene.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success is defined as a significant increase in the following areas:
   i. Increase to the number of cybersecurity clubs throughout Indiana middle and high schools (anticipated 130% growth within two years).
   ii. Increase the number of students registered in the clubs.
   iii. Number of cybersecurity camps conducted; there are zero in Indiana currently.
   iv. Number of industry certifications awarded to high school students.
   v. Establishment and success of statewide competitions.
   vi. Number of underserved and underrepresented students choose cybersecurity careers.
   vii. Number of students who successfully complete higher education career goals (two or four-year degree).
   viii. Number of participants in cyber apprenticeships, internships, and co-ops.
   ix. Number of participants who moved from any of the programs sponsored, as detailed by this document, and employed in a cyber-job in Indiana.
   x. Reduction in the number of job openings that cannot be filled (for example, determining if is there a decrease in the number of unfilled cyber positions as a result of these programs).

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes

b. **If Yes, please list states/jurisdictions**
   i. Indiana has created a similar program focusing on robotics; however, it does not include industry certifications.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Ability to procure funding match from government, industry, and private entities.
b. Funding for K-12 and higher education to continue to support the programs once implemented.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. It is anticipated that this initiative will become self-sustaining.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. The coalition for this initiative currently includes 40 formal partners at the local, State, and national levels.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. This initiative will demonstrate leadership from DWD, DOE, Academia and Industry engaged with the IECC.

Evaluation Methodology

Objective 1: Establish and fund a statewide cybersecurity program centered for K-12 stakeholders by July 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Launch a statewide cybersecurity program centered for K-12 stakeholder by August 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Job Demand Tool

Deliverable: Job Demand Tool

General Information

1. **What is the deliverable?**
    a. Proposal to modify and adopt Cyberseek as the source for cybersecurity-related job demand. The work group recommends infusing the Cyberseek tool with Indiana specific job demand, among other requirements, to assist Indiana job seekers and employers make more informed decisions.
    b. IN CyberPath will co-develop the Cyberseek tool for Indiana with an education portal that identifies all educational resources in the state and those that map to the NICE Cybersecurity Workforce Framework. The tool will have data analytics portal for industry to access their current workforce and for predicting future needs based on the NICE Framework. The Job Demand Tool will be designed for educators of cybersecurity to input data on the number of students enrolled in cybersecurity education for collecting metrics. Once completed, the mapping will allow for the council to determine the gaps in education, number of students being educated, and plan for future development of curricula through collaboration with providers.

2. **What is the status of this deliverable?**
    a. Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Will provide all stakeholders (state agencies, educators / training providers, employers) a single-source for cybersecurity-related job demand and education resources in Indiana. This will include the emerging skills, certifications, educations, etc. that employers are looking for from potential job candidates identified through the tools assessment portal. This can then be one additional tool that educators and training providers use as they assess how many cybersecurity-related offerings they provide and the required content that is mapped to the NICE Framework. The tool will also provide a portal for professional development for teachers and access to curricula for K-12.

6. **What metric or measurement will be used to define success?**
    a. Ability of the State to fill the demand for cybersecurity-related jobs. We will work with DWD to design a measurement tool that would include using data from Burning Glass identifying average days to fill cybersecurity-related jobs.
    b. Determine gaps in educational curricula needed across the state which will allow for the committee to plan to fill the gaps and address the lack of educational resources.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Employers, students, job seekers and educators

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Bureau of Labor Statistics occupation projections.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. IN CyberPath (Purdue University and Indiana University)
    b. Burning Glass
    c. Public-private partnership proposed via Cyber Economic Development Committee

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. DWD, DOE, CHE, Burning Glass Technologies, IN CyberPath, Cyber Leadership Alliance, Public-private partnership (see above), Purdue University, Indiana University, Ivy Tech Community College

12. **Who should be main lead of this deliverable?**
    a. DWD – R&A Team
    b. IN CyberPath Team

13. What are the expected challenges to completing this deliverable?

a. Building out the required data gathering and technology solution(s) to incorporate Indiana specific data to integrate with Cyberseek and IN CyberPath.
b. Incorporating Cyberseek job demand data and IN CyberPath educational resources tool and assessment portals into our existing eco-system of jobs / workforce data while ensuring data consistency and a cohesive user experience.
c. Marketing/promotion and training for use of the tools and programs

Implementation Plan

14. What is the deliverable?

a. Implementation plan to, modify, and adopt Cyberseek and IN CyberPath as the source for cybersecurity-related job demand and educational resources and assessments for career pathways for Indiana. The Cyberseek data and website can then be enhanced with Indiana specific data pertaining to job demand and salary.

15. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Procure Cyberseek for Indiana	DWD	0	2019	Awaiting costs/license fees for tool
Procure statement of work from IN CyberPath to provide mapping of state educational recourses and development of the assessment tool for industry				
Develop IN specific data for integration with Cyberseek	DWD	20	2019	
Enhance Cyberseek with Indiana Data from IN CyberPath	DWD	0	2019	
Develop integration plans for consumption of the Cyberseek data across various job seeker, employer, and education platforms utilizing sources from IN CyberPath.	DWD/DOE	0	TBD	Explore how cyberseek will be accessed. (example: direct links and/or API feeds into partner systems.)

Resources and Budget

16. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1	0.25	Project manager	State		
1	0.5	Data analyst	State		Data ETL, curation
0.5	0.5	Dev Engineer	State		Software automation
1		Systems analyst	State		Requirement/tech writing/testing

17. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Data/Compute server	Compute IN specific data	$10k				
Job Scheduler	Automation engine	$1k				

Benefits and Risks

18. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Cyberseek and the build out with IN CyberPath is a ready-made powerful tool that can be used by employers, educators, policy makers, and job seekers looking to understand cybersecurity-related jobs data within their geographic metro area. Adopting this tool will consolidate our collective efforts and understanding of cybersecurity-related jobs and their corresponding skill needs.

b. Infusing the Cyberseek tool with Indiana specific data and build out with IN CyberPath data and portals will further enrich the tool with data relevant to Indiana job seekers. Enabling better, more informed decisions as they consider cyber pathway options and cybersecurity needs.

19. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Informing users of employer needs and available openings. The tool can help reduce talent gaps and help direct the supply of cybersecurity workers.

20. What is the risk or cost of not completing this deliverable?

a. The risk is continued misalignment between employers, job seekers, policy makers, and training providers. Without the adoption of this tool, these constituents will continue to seek information about cybersecurity jobs from multiple sources which can and often does lead to misunderstanding of the cybersecurity job demand. This tool will also ensure that the State is aligning with the federal Cybersecurity Workforce Framework developed by NICE.

21. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Reduction in average time to fill for cybersecurity jobs.
b. Measurements of hard-to-fill and expensive-to-fill metrics for these jobs as sourced from Burning Glass technologies and employer feedback.
c. Number of educational recourses in the State for cybersecurity,
d. Gaps in education that exist.
e. Assessment of industry needs for cybersecurity workforce.
f. Level of cyber and general computer science understanding and skills.
g. Number of teachers getting instruction in cyber and computer sciences.
h. Number of cyber internships, apprenticeships, and co-ops at baseline.

22. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

23. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

24. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The data and software is proprietary and may be subject to scrutiny as competitors enter the market.
b. Understanding the Return on Investment (ROI) across the various constituents may be uncertain as it will take time to measure.

25. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. To the extent Indiana adopts Cyberseek as the tool to better understand cybersecurity jobs and skills needed to fill those jobs, then policy could be updated to reflect that

26. What will it take to support this deliverable if it requires ongoing sustainability?

a. A commitment to the tool, or comparable one in the future, as a guide to understanding cybersecurity jobs and the skills needed to fill those jobs.
b. Received a plan from IN CyberPath for the mapping and assessment portions of the tool.

27. Who has the committee/working group contacted regarding implementing this deliverable?

a. We have reached out the Burning Glass technologies with initial cost estimates for licensing.

28. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. Since career pathway options are illustrated in this tool, then individuals from other sectors looking for a job could benefit by using this tool. Common feeders include legal and business administration (auditors, financial analysts, etc).

Communications

---

29. Once completed, which stakeholders need to be informed about the deliverable?

a. DWD/DOE/CHE

30. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

31. What are other public relations and/or marketing considerations to be noted?

a. Some competing data providers may develop a similar tool with a focus of cybersecurity-related jobs.
b. As always, and in particular if or when this happens, Indiana will need to be prepared to defend the use of this tool along with the information coming out of it as competitors may raise concerns about the information and lobby for their tool/data to be used instead.

Evaluation Methodology

Objective 1: State of Indiana adopts Cyberseek as the source for cybersecurity-related job demand and career pathways for the state by August 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: State of Indiana will develop integration plans for consumption of the Cyberseek data across various job seeker, employer, and education platforms by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: K-12 Offering Cybersecurity Content

Deliverable: K-12 Offering Cybersecurity Content

General Information

1. **What is the deliverable?**
    a. Proposal to ensure an appropriate level of cybersecurity content is included in K-12 computer science offerings (per the Governor's Next Level Plan) and other initiatives, as appropriate (e.g. Hour of Code). On the one hand, this deliverable could be as simple as adding a layer of coordination across existing initiatives. On the other hand, it could be as expansive as creating formal expectations about cybersecurity in the K-12 curriculum with clear connections between the knowledge and skills students should have, when they should have them, and how they can be obtained.
    b. Identify, map and vertically align cybersecurity curricula to state and national standards.
    c. Pilot and scale up IN Cyberpath programs for P-16 and other postsecondary programs to increase student content knowledge and experience in cybersecurity.
    d. Create access and opportunity for underserved and underrepresented populations
    e. Increase the number of individuals going into cybersecurity jobs

2. **What is the status of this deliverable?**
    a. In-progress; 25% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Ensures that Hoosiers get exposure to Cybersecurity concepts early. This knowledge will help them decide if they might be interested in pursuing further education and a career in cybersecurity. At a minimum, this makes people more aware of good cybersecurity practices that will benefit them their entire life. The concepts relevant to cybersecurity in the workforce should be mapped back to the K-12 curriculum including broadly relevant content at early grades that would provide foundational understandings, dispositions, and skill development necessary to more focused skill development at the middle and high school levels.

6. **What metric or measurement will be used to define success?**
    a. Number of programs statewide offering with verifiable alignment to cybersecurity concepts and content.
    b. Scope and sequence showing development/articulation of cybersecurity concepts across grades K-12.
    c. Increase in professional development for teachers at all levels.
    d. Development of computer science strategic plans by schools with particular emphasis on the growth and development of students with strong preparation in cybersecurity.
    e. Number of postsecondary courses stood up that allows individuals to receive badges or certificates for indicating course completion.
    f. Number of individuals receiving badges or certificates from completing cybersecurity classes (post graduation)
    g. Number of individuals participating in educational and experiential programs

7. **What year will the deliverable be completed?**
    a. 2023+

8. **Who or what entities will benefit from the deliverable?**
    a. The workforce would be the ultimate beneficiary of this long-range development.
    b. Near-term, students would benefit from more opportunities for science attainment.
    c. Underserved and underrepresented populations will be more evenly represented in STEM careers.
    d. Could also be some benefit of a more informed citizenry—from the more intentional inclusion of cybersecurity in the K-12 curriculum.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Any funding targeting the development of STEM programming at the K-12 level.

Additional Questions

10. What other committees and/or working groups will your team be working with to complete or plan this deliverable?

a. No plans for work with other groups at the moment. This deliverable will require substantial vision and investment from policymakers and will take years to implement.
b. IN CyberPath via Purdue University and Indiana University

11. Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?

a. DOE along with those who provide content/training for the proposed K-12 computer science offerings across the state.
b. IN CyberPath Team
c. NICE
d. Burning Glass
e. Because of the scale of the work, there could be many contributors but there must be a goal, a shared vision, and an organization anointed to lead the charge.

12. Who should be main lead of this deliverable?

a. IDOE
b. IN CyberPath team

13. What are the expected challenges to completing this deliverable?

a. Ensuring that consistent (and correct) content is included in all of the various offerings/programs statewide.
b. Training teachers
c. Identifying funding
d. Writing curriculum and balancing the proposed additions with other content areas vying for attention within the K-12 curriculum.
e. Integrating cybersecurity curriculum into existing classroom practices
f. Statewide implementation

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Increase the number of schools certified through Common Sense Media to 200.	IDOE	80%	Fall 2019	16-17 school year there were 167 Indiana Schools Certified (https://d1e2bohyu2u2w9.cloudfront.net/education/sites/default/files/certified_schools_16_17_final.pdf) There were
Develop K-12 appropriate emphasis for Cybersecurity Month in October	IDOE	0%	October 2018	Could use the cybersecurity month as a platform for promoting an array of options for schools.
Develop an annotated curricular resources hub for K-12 teachers	IDOE	0%	September 2019	This could be at least partially met through the new CyberSecurity programming to be launched by the IDOE.
Develop and implement IN CyberPath	IN CyberPath	0%		This is a three phase program. Phase one include focus groups and development of the cyberseek took for Indiana. Phase two implements pilot programs both K-12 and CareerMakers. Phase three rolls programs out full scale across state.
Identify links between the professional development Code.org is offering to Indiana teachers and the cybersecurity domain.	IDOE	0%	September 2019	
Promote the development of a Cybersecurity Graduation Pathway	SBOE	0%	TBD	The State Board of Education has a process for reviewing Locally Created Pathways as part of the programming they are developing around Graduation Pathways.
Pilot Beta Offering of PLTW CyberSecurity course for 10th graders	IDOE	10%	September 2018	IDOE to fund participation by up to 10 schools interested in piloting this course.
Pilot phishing simulations with students through the state procured platform (Media Pro)	IDOE	0%	September 2019	IDOE is working to make the MediaPro platform available to all Indiana Schools. This platform includes access to a phishing simulation and training content.

Create and adopt a formal set of standards for cybersecurity across the K-12 curriculum	IDOE	0%	September 2019	This is a big lift but would really help to lay the foundation for moving from the piecemeal approach we have now to a more full-court press so all students have basic awareness and understanding about cybersecurity matters—a new essential skill to be an educated citizen.
Create cybersecurity summer camp for k-12 students.	IU	90%	Summer 2018	Indiana University will run the Security Matters Cybercamp for interested students from throughout the state and use the workforce development subcommittee to help promote the camp.
Create CareerMaker course for post-secondary training, offering certificates and/or badges for completion.	IN CyberPath Team	0%	TBD	This is part of the IN CyberPath project with Purdue and IU

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1.0	1.0	Management coordination, advocacy	State		There are bits and pieces of the tactics enumerated above that are already underway, what is needed is an individual who has the coordination and expansion of these efforts as a primary responsibility.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Consultation	Guidance and project management to develop Cybersecurity standards for K-12	TBD	TBD	State/Federal	grants	
Travel	See exemplar programs in action in other locations.	TBD	TBD	State		
IN CyberPath framework	Cyberseek tool developed for Indiana	TBD	TBD	Grants	Industry donations	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The most important benefit of this deliverable would be the coordination of disparate efforts and the contribution that coordinated efforts could make toward keeping the pipeline of talent full.
b. A statewide cybersecurity interactive tool for Indiana
c. Industry-aligned post-secondary student programs at Purdue University's CareerMakers sites.
d. And assessment tool for collecting metrics from industry

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This would reduce the cybersecurity risk or impact in two ways
    i. Ensuring that all students receive basic exposure to cybersecurity content throughout their time in Indiana schools. We rely on schools to create an educated citizenry. We need our citizenry to have awareness of cybersecurity topics and challenges that is developmentally appropriate.
    ii. Provide aligned exposure to cybersecurity topics throughout the K-12 curriculum including both formal and informal learning opportunities so that more students will consider careers in the area of cybersecurity.
    iii. Provide the opportunity for individuals in the workforce to increase their knowledge in cybersecurity and job opportunities by furthering their education.

19. What is the risk or cost of not completing this deliverable?

a. The risk is having uncoordinated investment in many good things that could have greater effect if considered together. Also, if there is no real attention given to cybersecurity awareness and training at the younger ages of the spectrum, we will have to keep putting out fires and being reactive to real and immediate shortages in the job market.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. A clearly articulated cybersecurity program for K-12 that shows the critical path and skills for cybersecurity and how various opportunities, experiences and curricula can fulfill those critical needs. In addition, optional extensions of core concepts in cybersecurity should also be articulated. Indiana should have a clear map of critical cybersecurity content that clearly shows what topics will be encountered at what ages.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. Indiana would be among the first to implement a cybersecurity curriculum or even to map cybersecurity concepts across the curriculum.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. This thinking requires a long view.
b. The actual return on investment is not as direct as some may like.
c. Any results with direct impact to the economy are years away.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. The policy change here would be a formal expectation regarding content and skills about cybersecurity that should be encountered during the K-12 experience.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. An ongoing commitment to revising and amending the cybersecurity curriculum to keep it relevant and responsive to the needs of the workforce and to the needs of society as a whole.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. No formal contacts have been made regarding a coordinated effort on this front although members of the committee are aware of episodic efforts underway.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. If this deliverable is well-executed, other sectors could experience direct and indirect benefit

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. K-12 Schools

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes
b. If formal steps were taken in this area, it should definitely be part of the overall effort outlined on the cybersecurity web site.

30. What are other public relations and/or marketing considerations to be noted?

a. Not all families welcome the use of computers in the classroom and some resist the provision of devices to students. If cybersecurity becomes a curricular emphasis, there will need to be some care given to the education of parents who are concerned that their children are safe and are also concerned about the age-appropriateness of what they know about cybersecurity threats.

Evaluation Methodology

Objective 1: Indiana Department of Education will develop a menu of cybersecurity content and initiatives that includes K-12 computer science offerings by September 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Eighty percent of Indiana Schools adopt one or more cyber initiatives by August 2020.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

☐ Peer Evaluation/Review

Deliverable: Best Practices and NICE Framework Standard

Deliverable: Best Practices and NICE Framework Standard

General Information

1. **What is the deliverable?**
    a. Working with the Nationa Governors Association, the IECC Workforce Development Committee will develop a detailed implementation plan for Indiana adopt cybersecurity workforce best practices and standards, such as the National Initiative for Cybersecurity Education(NICE) Cybersecurity Workforce Framework, and provide tools to the full ecosystem of Indiana's workforce (K-12, educators, students, underemployed, employers, etc.).

2. **What is the status of this deliverable?**
    a. In-progress; 25% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. All entities will use the framework as a common language when describing cybersecurity-related jobs, skills, knowledge, abilities, and tasks.

6. **What metric or measurement will be used to define success?**
    a. Ability of the State to fill the demand for cybersecurity-related jobs. We will work with DWD to design a measurement tool that would include using data from Burning Glass identifying average days to fill cybersecurity-related jobs. Determine what educational resources exist that are mapped to NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework.
    b. Determine what gaps exist in education and curricula.
    c. Ability to assess the needs of industry related to the number of employees that currently exist and future needs based on advancement of technology.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Any that need to develop cybersecurity-related job description, education curriculums, apprenticeships and resumes. This includes at least: job seekers, educators/training providers, and employers.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Potentially, any entity with adoption of other NIST standards.

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Any entity or group necessary to codify this adoption.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. DOE, DWD, CHE, NIST

12. **Who should be main lead of this deliverable?**
    a. DWD

13. **What are the expected challenges to completing this deliverable?**
    a. Providing various tools to allow users to more easily utilize the framework. Research ongoing to determine priority for what tools may be needed (e.g. job description writing tool) in conjunction with the NICE consortium of various state reps and NGA. Developing curriculum to describe and teach the knowledge, skills, and abilities (KSAs) and Tasks as outlined within the NICE Framework.

Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. On-going Deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Begin implementation planning for making NICE the standard across Indiana	IECC Workforce Development Committee / National Governors Association (NGA)	100%	August 2018	See Supporting Documentation for NGA Workshop Materials.
Create and implement statewide outreach program for cybersecurity training that follows best practices and standards, such as the NICE Framework, to underserved communities, minorities, women, veterans, disables, and minor offenders	IECC Workforce Development Committee/NGA	20%	December 2019	
Create and implement statewide program that will provide educators and businesses resources for meeting best practices and standards, such as the NICE Framework, by December 2019.	IECC Workforce Development Committee/NGA	20%	December 2019	
Procure statement of work from IN CyberPath to provide mapping of state educational recourses and development of the assessment tool for industry	Partners	20%	2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. [No Response]

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. [No Response]

19. What is the risk or cost of not completing this deliverable?

a. According to DWD, Indiana needs to fill more than 1 million jobs over the next decade. Of those million jobs, more than a third will be new or growth occupations within the state.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. [No Response]

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. [No Response]

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. [No Response]

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. [No Response]

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. [No Response]

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All sectors benefit from this initiative.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None at this time.

Evaluation Methodology

Objective 1: Indiana formally establishes NICE Framework as the cybersecurity standard for the state by October 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Working with the National Governors Association, the IECC Workforce Development Committee will create and implement statewide program that will provide educators and businesses resources for meeting best practices and standards, such as the NICE Framework, by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 3: Working with the National Governors Association, the IECC Workforce Development Committee will create and implement statewide outreach program for cybersecurity training that follows best practices and standards, such as the NICE Framework, to underserved communities, minorities, women, veterans, disables, and minor offenders by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Incentivized Cybersecurity Certifications

Deliverable: Incentivized Cybersecurity Certifications

General Information

1. **What is the deliverable?**
    a. Utilizing the NICE framework, provide incentivized cybersecurity certifications to industry across the State of Indiana. This initiative will provide a minimum of 200 industry certifications within two years. On average, certifications will be provided at a 50% cost savings.
    b. Goals:
        i. Create statewide cybersecurity certification training program
        ii. Reduce barriers to entry for cybersecurity education to individuals & Indiana businesses
        iii. Create access and opportunity for underserved and underrepresented populations
    c. IN Cyberpath will utilize resources from Purdue University, Indiana University, Vincennes University, Ivy Tech, and other state institutions of higher education to develop the curriculum for cybersecurity certificates under the IN Cyberpath program.

2. **What is the status of this deliverable?**
    a. In-progress 75%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. All entities will use the framework as a common language when describing cybersecurity-related jobs, skills, knowledge, abilities, and tasks.

6. **What metric or measurement will be used to define success?**
    a. Ability of the state to fill the demand for cybersecurity-related jobs. We will work with DWD to design a measurement tool that would include using data from Burning Glass identifying average days to fill cybersecurity-related jobs.
    b. Fully developed IN CyberPath Framework is adopted by state and used by educators and industry.
    c. K-12 schools across the state offer cybersecurity courses that align with IN CyberPath framework.
    d. CareerMakers have cybersecurity courses stood up across the state that aligns with IN CyberPath framework.

7. **What year will the deliverable be completed?**
    a. 2019
    b. 2019 for IN CyberPath phase one, 2021 for phase two and 2025 for phase three

8. **Who or what entities will benefit from the deliverable?**
    a. Any that need to develop a cybersecurity-related job description, education curriculums, and resumes. This includes, at least, job seekers, educators, training providers, and employers.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Potentially any entity with adoption of other NIST standards.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Any entity or group necessary to codify this adoption.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. DOE, DWD, CHE, NIST
    b. Purdue University, Indiana University, Burning Glass

12. **Who should be main lead of this deliverable?**
    a. DWD

13. What are the expected challenges to completing this deliverable?

a. Providing various tools to allow users to more easily utilize the framework. Research ongoing to determine priority for what tools may be needed (e.g. job description writing tool) in conjunction with the NICE consortium of various state reps and NGA. Developing curriculum to describe and teach the KSAs and Tasks as outlined within the NICE Framework.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. One-time deliverable (two-year program)

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Preparation and Planning	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	80%	Award of Funding (A)+1	
Identify Candidates	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	50%	A+2	Cummins, KAR, Wabash, Rofori, etc.
Form first 4 cohorts (G1)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+3	
Finalize Regional Locations	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	80%	A+4	Select university locations statewide
Train First Cohorts (G1)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+6	
Progress Review & Refinement	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+7	
Form Second Cohorts (G2)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+8	
Train Second Cohorts (G2)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+10	

Form Third Cohorts (G3)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+13	
Train Third Cohort (G3)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+17	
Form Forth Cohort (G4)	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+19	
Train Forth Cohort	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+22	
Review	IECC Subcommittee /Cyber Leadership Alliance Coalition (CLAC)	0%	A+23	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Line Item	Cost	Detail
Certification Camps	$451,000.00	All-inclusive certification boot camp (lab, exam voucher, materials, labs, instructor, facility). 16, 20-person cohorts for CISA, CISM, CISSP, CEH. 1, 11-person cohort for CIPP). Total 331 spots. Based upon DWD demand data and partner input.
Outreach	$50,000.00	Underserved community outreach, 5 groups: Women, Minority, Hispanic, Veteran, Disabled
Advertising	$20,000.00	Print, Video, Virtual ad space. Social media
Coordinator	$21,000.00	30% of full-time coordinator for implementation & integration
Project MGMT & Leadership	$39,000.00	30% of full-time project manager/senior consultant
Total	$581,000.00	
Private Match	($342,200.00)	CLA: $240,000 - curriculum development. Purdue: $23000 facility EC Council: $68000 vouchers. ISACA: $11,200 vouchers

- Funding sources: Request funding from State of Indiana with a significant match from private industry.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The initiative will deliver a potential economic impact of over $130 million from activities executed over the two-year period. This claim is based upon the results of the completed Outcomes Worksheet (originally submitted to the Skill-Up committee) with jobs data from Burning Glass and Indiana Department of Workforce Development (DWD). In addition to the significant economic impact by increasing the number of Hoosiers attaining high-paying jobs, making cybersecurity training available and affordable to small and medium-sized businesses reduces barriers to entry and reduces the largest cybersecurity risk surface. Not only will open job requisitions be filled, but it is projected that more companies will relocate high-paying cyber jobs to Indiana to capitalize on the enhanced talent pipeline.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Refer to previous questions.

19. What is the risk or cost of not completing this deliverable?

a. According to DWD, Indiana needs to fill more than 1 million jobs over the next decade. Of those million jobs, more than a third will be new or growth occupations within the State. As the nature of work continues to change at an accelerated pace, the workforce will need new skills to meet the challenge at all levels of education. It is estimated that nearly 30,000 job openings per year will require an industry-recognized certificate/certification in addition to a high school diploma. Indiana will continue to leave approximately 2,500 cybersecurity jobs statewide unfilled creating an incalculable risk to industry, wealth, and the citizenry.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success will be measured by using metrics from CyberSeek/Burning Glass/DWD. Currently, there are 1,606 Indiana jobs posted requesting six different cybersecurity industry certifications. This initiative is estimated to conservatively provide over 200 certifications over the next 2 years reducing the demand by a minimum of 14% across the State.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The ability to secure funding.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. It is anticipated that this initiative will become self-sustaining by the end of the initial 2-year funding period.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. The coalition for this initiative currently includes of 40 formal partners at the local, State, and national levels.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All sectors benefit from this initiative.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Marketing assets from CLAC partners will be leveraged to ensure the success of the program.

Evaluation Methodology

Objective 1: Indiana Department of Workforce Development and partners will create and launch statewide cybersecurity certification training program that meets best practices and NICE standards by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Program Data Tool

Deliverable: Program Data Tool

General Information

1. **What is the deliverable?**
    a. Develop mechanism to gather data on all cybersecurity programs and offerings across the state and the number of participants. A report on the students that are attending Indiana public, private, and for-profit post-secondary institutions in cybersecurity related fields so that the Indiana Executive Council on Cybersecurity can more fully understand the supply of qualified graduates and their credentials/degrees to make better informed policy decisions. A goal would be to collect Major and Minor-level data.
    b. Use the cyberseek portals to collect and analyze data to iteratively develop IN Cyberpath programing.

2. **What is the status of this deliverable?**
    a. In-progress 25%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Will provide the state the ability to see all available programs and the number of people that are current in the "pipeline". This information along with the information from the Job Demand Tool proposal will allow stakeholders to understand if the state is producing enough skilled people to meet the anticipated demand.
    b. This tool will be used as:
        i. Portals for primary to secondary teachers, instructors and students with Career Pathways, curricula, project based resources.
        ii. Recourses for teachers related to Professional Development.
        iii. Assessment tools for companies, employees, government for assessing cybersecurity aptitudes and abilities of employees.
        iv. Apprenticeships programs for preparing the cybersecurity workforce.
        v. Identify co-op and internship programs available across the State.

6. **What metric or measurement will be used to define success?**
    a. Ability to accurately measure (e.g. ensure data available from public institutions, 3rd party training providers, and private institutions).
    b. Number of hits on the website portal.
    c. Number of apprenticeship programs stood up.
    d. Number of coop and internship programs.
    e. State science test scores related to cybersecurity/computer science.
    f. Number of companies participating in the programs.

7. **What year will the deliverable be completed?**
    a. 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Having a pipeline report on cybersecurity degrees and certifications that is complete and well-trusted could be a tool of economic development and could make Indiana more attractive to business wanting to locate to the state.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State and federal programs aimed at developing capacity in cybersecurity and related fields would advocate for this data.
    b. Not sure if other states face similar reporting challenges in the area of majors vs. areas of academic emphasis.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The workforce group is currently not coordinating with other committees on this deliverable.
    b. IN CyberPath team (Indiana University and Purdue University)

11. Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?

a. CHE
b. DWD
c. Indiana Management Performance Hub (MPH)
d. Purdue University
e. Indiana University

12. Who should be main lead of this deliverable?

a. CHE

13. What are the expected challenges to completing this deliverable?

a. Gathering accurate data (without significant effort) across all of the providers/educators. And being able to do it periodically.
b. We don't want this effort to be a labor-intensive survey each time data is needed. There is an existing process for data gathering from public higher education institutions that can be utilized for that segment of providers.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
CHE Policy & Research Team meet with Institution Research Teams	Michael Hawryluk	50%	April 2018	Meeting is/was scheduled for 4/11/2018.
Develop Initial Survey for Institutions to Report Cybersecurity related students/degrees/programs	CHE	0%	TBD	
Analyze/Synthesize Data from Institutions on Students/Degrees/Programs and Develop Report on Findings	CHE	0%	TBD	
Develop Ongoing Plan for Future Recurring Collection	CHE	0%	TBD	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0.15		Data Analysis			This effort will be to develop the survey, analyze/synthesize the results and provide a report to the IECC. This can likely be accomplished using existing Exempt FTE/Staff. Depending on the ongoing requirements of collecting this data regularly, this is subject to change.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. This can be accomplished using email and productivity software (e.g. Excel, Word) for the near-term collection. Depending on the ongoing efforts, additional resources or modifications to existing software systems may be required.

b. Software as related to the Cyberseek tool.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Regularly reported data on supply of cybersecurity-related degree seekers and completers will give the IECC the insight into the supply-side of the equation for post-secondary institutions to understand if policy changes are necessary.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Our ability to insource cybersecurity expertise will provide less financial risk as we will be better able to recruit graduates from Indiana colleges to work for Indiana companies.

19. What is the risk or cost of not completing this deliverable?

a. If we don't know the supply-side of the equation, we may have to outsource cybersecurity jobs/contracts to other states, countries and/or have to pay higher prices/premiums to accomplish necessary work. If we are unable or unwilling to pay for this work, the State of Indiana and its businesses may be subject to additional risk.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. We need to have major-level data on cybersecurity-related degrees. We currently do not have major-level data.
b. Minor-level data would also be helpful to understanding the supply.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. If additional deliverables are placed on staff slated to work on this, it could move the timeline back or risk causing other deliverables to slip in schedule. Having additional resources available would mitigate this, especially for the analysis/report writing part. Potentially, we should have available resources across the entire IECC that can assist in these tasks for various sub-committees and working groups.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. We may want to require Institutions to report more granular data than degree-level. This could be codified, but likely will require much deeper conversations than have been had at this point.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. To support this deliverable in the future, CHE will need to modify its CHEDSS system to account for major-level data and Indiana post-secondary institutions will need to modify their processes to report on these data. It's unclear what the exact effort or financial implications of these changes will be.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. At this point, the implementation of this deliverable has been discussed internally at CHE at least through the collection of the data. Staff at CHE has contacted research teams at some Indiana public institutions to determine the feasibility of collecting major-level data and the initial result was positive. Now, we need to develop a survey, send it out, and report on the findings.
b. IN CyberPath

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. If we do expand the collection of this major-level data to non-cybersecurity fields, it could potentially be used by a multitude of additional sectors.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Indiana post-secondary institutions should be notified regarding the output of the deliverable.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None.

Evaluation Methodology

Objective 1: Indiana Commission for Higher Education will develop and launch survey for post-secondary to report on cybersecurity-related programs by March 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indiana Commission for Higher Education will develop and deliver a final report to the IECC on findings of post-secondary survey by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- National Governor's Association Policy Academy – Indiana 1st Workshop Notes August 2018

National Governor's Association (NGA) Policy Academy

Indiana 1st Workshop Notes

August 2018

August 22: Cybersecurity Workforce Development

Panel 1

Rodney Peterson, NICE

- Need to make sure we are reaching out to all populations: women, minorities, veterans
- There is an online tutorial on how to use the NICE framework
- Main goal is to have a common language that everyone can use
- Can work with Cyberseek to see where the NICE framework aligns to the current job openings
    - Also contains information on how many individuals have specific certifications and how that aligns to specific NICE positions

Stephen Schneiter, COMPTIA

- Need to work with K-12 more so that they understand the certificates that are needed for employment opportunities
- El Paso Texas case study
    - Trained veterans on security certifications
    - All of them who went through the program became employed
- Cannot overlook the end-users. Cybersecurity starts with the end-users
- Really a need for basic awareness/cybersecurity training

Sarah Benczik, Deloitte

- Talent Lifecycle: There is a workforce that is available; then there is an analysis of who we need to bring into the organization and who we currently have in the organization; then organizations start recruiting; once employee is in the organization, there is skill development (skills are only as good as 3-5 years); then you have performance management so that employees understand what is expected of them and what kind of skills they require; and then employees know where to go for the rest of the day. The NICE framework follows this track and allows employees and organizations to easily

Josh Drumwright, Deloitte

- How do we perform work more efficiently
- Started a gig system: identifying tasks that could be outsourced;
- Having a passion for the subject is very important; thinking more broadly on how to bring in the people you need to address those challenges
- How do you revision the work and scope it broader so that you are appealing and finding the best applicant pool

Q&A

- The framework is still a work in process;
- Don't want to have a compliant exercise in which you simply check the box of the qualifications that you need; but how you can use those qualifications to overcome the risks
- The Framework helps to accelerate your workforce; the challenge is that the Framework has a lot of detail

- Encourage using the common vocabulary
- Need to encourage hands on learning/experience based learning
- Worry about the NICE framework becomes a certification/compliance factor. Don't want to say that because we have the NICE framework implemented we are secure

- What are the barriers
    - High school and community colleges are very attuned to getting their students jobs, so the buy-in is very high. But there are universities that are more concerned about life long careers as opposed to just a "job." So the language needs to change to account for that
        - Teach people about how to think intellectually;
    - Need to prepare people how to be lifelong learners because they will need new certifications
    - There are always constant needs or gaps that are changing; need for strong skillset and managers to work with the current workforce on how they can improve, the skills they need to improve, and the organization can help them. Need to ensure that you don't shirk managerial skills
    - Need to get over the feat that training leads to mobility because it will be worse if they stay and don't get trained
- Did you subscribe to a framework to create the NICE Framework?
    - This was a community activity
    - A lot of focus groups and existing materials that we used.
- Have you seen examples of universities using apprenticeships?
    - These are very important for students and workers to accelerate the trainings/knowledge
    - A lot of organizations are sponsoring cyber competitions
    - Crowdsourcing is becoming very popular
    - California: have a lot of businesses working with High school

Facilitation: First Session

Group 1 First Session: Employers

1. What are the tasks that your organization needs to perform its mission?
    a. Educating non-specialists (cyber hygiene)
    b. Supply chain management
    c. Foster research and education in cybersecurity
    d. Hands on experience
    e. Planning for the future
    f. Data identification and classification
    g. Recruitment strategies
    h. Winning leadership buy-in
    i. Building awareness
    j. Creating talent pipeline (including internal skill development)
    k. Career education
    l. Information system acquisition
    m. Evidence-based strategic planning

   n. Threat modeling
   o. Performance development
   p. Organizational change management
   q. Security for financial aid distribution (for schools)
   r. Hardening of hardware
2. What are employees' knowledge, skills, and abilities (KSA) strengths to perform those tasks?
   a. Hands on experience
   b. Human/behavioral focus
   c. Creative thinking
   d. Cyber intelligence analysis
   e. System perspective
   f. Knowledge of the difference between risk and security
   g. Ability to "think in the grey"
   h. Threat modeling
   i. Data analysis and business context
   j. Knowledge to navigate issues/concerns
   k. Understanding of hardware
   l. Understanding the entire stakeholder ecosystem (outside of organization)
   m. Knowledge of security by design
   n. Mentality for lifelong learning
   o. Soft skills
   p. Data science

Group 2 First Session: Employers

1. What are the tasks that your organization needs to perform its mission?
   a. Defend the network
   b. Knowledge on the need to defend the network
   c. Identify risks and intelligence gathering
   d. There is a need to identify the spectrum of roles needed and which roles and responsibilities can be outsourced
   e. Educational institutions need to identify the skills needed to teach students
   f. Threat assessments
   g. Need a sector driven cybersecurity education development
   h. Need to message why cybersecurity is important
   i. Employees need to report suspicious activities
   j. Auditing vendors
   k. *Unrelated thought: need to make sure the message is being pushed down to locals*
2. What are employees' knowledge, skills, and abilities (KSA) strengths to perform those tasks?
   a. Difficult to assess because there are shifting priorities
   b. Need to react to unplanned circumstances
   c. Meet the need of stakeholders
   d. Ability to pivot
   e. IT personnel are very responsive to customer requests

Our conversation started to discuss overall weaknesses and what organizations would like to see:

- Need to convey that cybersecurity is everyone's problem

- The state should host cyber boot camps for teachers to teach them on Cybersecurity 101 to effectively teach students
- Need to teach about the ethics of cybersecurity. This should be a priority and not an afterthought
- In order to attract more women and girls to cybersecurity, we should message it as a "protector" role
- If we institute the NICE framework and adopt their credentials, we have to make sure we avoid complacency
- Need to emphasize and invest in continuing cybersecurity education and credentialing
- We have to make sure that we convey how these skills are adaptable and transferable
- There is a lack of investment in trainings
- Lack of record/performance management on what credentials/trainings are better than others
- IT needs to be proactive instead of reactive and we need to learn from attacks
- IT responsive
- We need a culture change to highlight that cybersecurity cross-cuts all industries. Just because you get a degree/certificate in cyber, doesn't mean you have to go to an IT industry. You can work for a hospital or nonprofit to practice your education. Likewise, we need to think about how to recruit individual's with non-IT backgrounds into cybersecurity roles because they are just as valuable
- Need to make sure don't rely on traditional IT degree/qualification
- Need to train service desk employees to talk about cybersecurity in layman's terms when talking with customers

Facilitation: Second Session

Group 1 Second Session: Students, Job Seekers, Workers

1. What factors inhibit/deter potential workers?
    a. Pay
    b. No clearance
    c. Remote working offered by companies on the coasts
    d. Company reputation
    e. Lack of awareness of possibilities in cybersecurity community
    f. Chicken and egg problem: companies ask for a lot of experience even for entry level positions
    g. Poor branding for the cybersecurity business
    h. Too much emphasis on 4 year degrees instead of skills
    i. Location, location, location
    j. Fear of math and computer skills
    k. Difficult for hiring managers to sell sensitive duties that they cannot discuss in detail
    l. People misunderstand what cybersecurity jobs entail
2. What encourage students/job seekers/workers to get involved or apply to jobs?
    a. Flexibility
    b. Seeing a career path that is NOT necessarily in management
    c. Pay

   d. Travel
   e. Illustrate the many journeys available
   f. Family
   g. Niche offerings
   h. Employer interest in employees' lives over their work product
   i. Access to resources/training
   j. Making cybersecurity sexy and meaningful
   k. Career development opportunities
   l. Seeing diversity, and people like them, in the industry
3. Why don't young people even consider cybersecurity?
   a. No cybersecurity pop culture for children
   b. We do not condition cybersecurity knowledge at a young age
   c. Lack of general education for consumers
   d. Terms like "security" turn people off early
   e. Cyber still taught as a separate subject—not integrated into normal curriculum
   f. Tangible examples of "cyber heroes" are not part of childhood
   g. No cybersecurity toolkits for teachers of very young students
4. Which promising talent is the community failing to reach?
   a. People who lack digital connectivity
   b. Non-cyber specialists who nevertheless have a role in cybersecurity
   c. Trained employees from the inside who understand the broader business context
   d. Non-cyber workers with an aptitude

Group 2 Second Session: Students, Job Seekers, Workers

1. What factors currently exist that inhibit or deter potential workers from applying to jobs or accepting job offers?
   - Gender bias profile
   - Companies need to articulate that their open job is cyber related. In other words, for those companies that are not traditional IT companies, they need to convey to cybersecurity professionals or students that they can utilize their skills at the company
   - This job is a high risk job with a lot of accountability; so there may be a fear that if a mistake is made, one can be fired very quickly
   - Work/life balance
   - There is a lack of clarity/expectations on what type of education requirements an applicant should have
   - Lack of diverse mentors
   - Need to make apprenticeships more accessible to minority communities and women
   - need to expand applicant pool by thinking about non-IT degrees
   - Currently, there is a belief that if I get this degree or that certificate in cybersecurity then I am restricting myself to a strictly cybersecurity career

2. What factors currently exist that encourage job seekers to apply or accept job offers?
   - Money
   - Altruism
   - Job mobility
   - Not a boring career

3. Other than money, what are "perks" that your organization could offer?
- The sense of mission
- National Guard can provide real world experience
- Placement rate/ability to get a job
- being part of a larger cybersecurity community

4. What are your current outreach efforts? Are there applicant pools you are not reaching? *(this conversation turned into outreach strategies we should consider creating)*
- Need to convey and develop a message on why cyber professionals should work in Indianapolis and that they don't have to move to San Francisco for work. This message could entail the salary purchasing power and cost of living comparisons between Indiana and San Francisco
- Need to increase awareness of associations/clubs/competitions for cybersecurity and their impact
- For K-12: To engage them and to show why cybersecurity would be an interesting career, create examples on the impact a cybersecurity event can have on their life (e.g. would be unable to go online and play videogames, access their favorite apps)
- For K-12, need to be explicit on what exactly cybersecurity is
- Engage teachers to develop cybersecurity curriculum in pre-existing computer science classes
- Need to identify potential federal funding to conduct outreach or to pay for these outreach initiatives
- Do a fieldtrip with teachers/students to the cyber range

Facilitation: Third Session

Group 1 Third Session: Educators/Trainers

1. What are current partnerships between educators and non-educators?
    1. Cyber Corps Scholarship for Service
    2. Retraining veterans with clearances
    3. Cooperative education programs
    4. Michigan's "Marshall Plan"
    5. Workplace Simulation Project
    6. Faculty-Designed Courses for Industry
    7. Employers getting into the classroom any way possible
2. How do current curriculums reflect employer's needs? If not, why not?
    1. By accident
    2. Field experience of the instructor
    3. Industry advisory boards to help design curriculums
    4. Faster approval of courses
    5. Lack of focus on non-cyber skills
    6. Industry does not know what they want
3. For non-educators, what education or training programs do they utilize?
    1. Offer free credentialing
    2. Job shadowing
    3. TIGS
    4. Align with client needs
    5. Train to compliance

6. Training on elements of general career success

4. For educators, do you have sufficient students enrolled in your programs? If not, what needs to be done to increase the student pipeline?
    1. Change the branding
    2. Emphasize problem solving
    3. Use influencers
    4. Tie into core introduction for new students
    5. More access to labs and hands-on equipment
    6. Emphasize the element of cybersecurity in maximizing personal SAFETY and HEALTH
    7. Explain that students really can be cyber warriors
    8. Consolidate all available resources into one place

Group 2 Third Session: Educators/Trainers

5. What are current partnerships between educators and non-educators?
    1. Cyber Start
    2. Cyber Siege
    3. Cyber Patriot
    4. Gen Cyber
    5. START Engineering
    6. NSA-CCEL
    7. NetSmart
    8. National Centers for Forensic Institute
    9. Grid-Ex
    10. Cyber Storm
    11. Need to engage and partner with the fusion center more
    12. Need to have more partnerships between industry and K-12 and to bring volunteers from industry to engage with students
6. How do current curriculums reflect employer's needs? If not, why not?
    1. Teachers and universities need to know what industry is training its employees so they know what to train students on
    2. Need to foster collaboration with other industries (e.g. health) to see if there are best practices within their curriculum that can be applicable to cybersecurity curriculum
    3. A huge weakness is that most curriculum haven't been tested or vetted, so we don't know if what we are teaching is useful/effective
    4. Have to make sure we are including ethics.
7. For non-educators, what education or training programs do they utilize?
    1. We need to make sure that employee trainings lead to credentialing
    2. Need to do a better job highlighting what type of trainings are available for workers
8. For educators, do you have sufficient students enrolled in your programs? If not, what needs to be done to increase the student pipeline?
    1. We have to be cognizant of teachers' capacities and realize that they are being asked to teach several different topics

<u>Facilitation: Fourth Session (Both groups combined)</u>

1. Employers
    a. Rewrite job descriptions according to NICE

   b. Tool for small businesses to design job descriptions
   c. Using NICE Framework to design performance management
   d. Share IBM/Purdue partnership successes
   e. Differentiate NICE Framework from Department of Labor categories
   f. Socialize NICE Framework with HR offices
   g. Develop incentives to encourage adoption of NICE Framework by smaller employers
   h. Use NICE Framework to organize companies/school discussions
2. Educators
   a. Incorporate risk management into curriculums
   b. Creating sector-specific instruction
   c. Expand academic advisory boards
   d. Process for developing aptitude testing
   e. Collect best practices on academic advisory boards
   f. Don't forget the business focus of cybersecurity
   g. Design attacker mindset into curriculums
3. Generate Interest
   a. Get commitment from IN companies for a PR campaign around cyber jobs
   b. Understand why underserved individuals are not engaged
   c. Assistance to offset time & money needed to retrain for cyber
   d. Naviance tool for cyber
   e. Popularize "cyber" heroes
   f. Use games relevant for cyber
   g. Layer degrees with certifications
   h. Roadshows are key—get to those who will not come to large convenings
   i. Get unemployment offices information on available resources
   j. Dual credit program for adults
   k. Create basic guide for those who know NOTHING
   l. Approach K-12 in different components (not as one block, but as low, mid, and high components)
   m. Veterans → trailing spouse (?)
   n. Incorporate cybersecurity into existing degree programs
   o. Align disabilities to NICE roles→involve appropriate advocacy organizations to promote the connections

APPENDIX D.11

CYBER PRE- & POST- INCIDENT WORKING GROUP

CYBER PRE- THRU POST- INCIDENT WORKING GROUP STRATEGIC PLAN

Chair: Major General Courtney Carr | Co-Chair: Dewand Neely

September 2018
Indiana Executive Council on Cybersecurity

Cyber Pre- thru Post- Incident Working Group Plan

Contents

Committee Members **4**

Introduction **7**

Executive Summary **9**

Research **12**

Deliverable: Exercise **16**

General Information 16

Implementation Plan 17

Evaluation Methodology 21

Deliverable: Cyber Emergency Response Team (IN-CERT) **23**

General Information 23

Implementation Plan 24

Evaluation Methodology 27

Deliverable: Gap Analysis **29**

General Information 29

Implementation Plan 30

Evaluation Methodology 33

Deliverable: Cyber Assessments **35**

General Information 35

Implementation Plan 36

Evaluation Methodology 40

Supporting Documentation **42**

Department of Homeland Security (USDHS) Sector Risk Snapshots 43

IECC Cyber Vulnerabilities Whitepaper Communications Sector 96

IECC Cyber Vulnerabilities Whitepaper Energy Sector 100

IECC Cyber Vulnerabilities Whitepaper Water and Wastewater Sector 104

IECC Pre- through Post-Incident White Paper Education Sector 108

Indiana National Guard (INNG) State Cyber Baseline Survey Results 115

Committee Members

Committee Members

	Name	Working Group Position	ECC Membership Type
	Dewand Neely	Co-Chair	Voting
	Courtney Carr (MG)	Co-Chair	Voting
	James Gordon	Advisory	Advisory
	Tim Winslow(COL)	Advisory	Advisory
	Jeff Hackett(COL)	Co-Chair Proxy	Voting Proxy
	David Tygart	Advisory	Advisory
Communications Sector - sub working group			
	Daniel J. Solero	Advisory	Voting Proxy
	Dave Skalon(LTC)	Voting	Advisory
Education Sector - sub working group			
	Andrew Korty	Voting	Advisory
	Matthew Etchison	Advisory	Advisory
	William Mackey	Voting	Advisory
	Chad Pollitt	Advisory	Advisory
	Darryl Togashi	Advisory	Advisory
	David Greer	Advisory	Advisory
Energy Sector - sub working group			
	Carl Cahill	Voting	Advisory
	Stanley Partlow	Advisory	Advisory
	Walter Grudzinski	Voting	Advisory
	Sarah Freeman	Advisory	Voting Proxy
Financial Sector - sub working groups			
	Seth Cooper	Voting	Advisory
	Owen LaChat	Voting	Voting
	Michael Servas	Advisory	Advisory
Government Law Enforcement - sub working group			
	Paul Dvorak	Advisory	Non-Voting
	John Davidson	Voting	Non-Voting
Government Services - sub working group			
	Thomas Vessely	Voting	Advisory
	James Haley	Advisory	Advisory
	Jeff Tucker	Advisory	Voting Proxy
	David Ehinger	Voting	Voting
Healthcare - sub working group			
	Frank Nevers	Voting	Advisory
	Mark Swearingen	Voting	Advisory
	David R. Day	Advisory	Advisory

Private Sector members			
	Landon Lewis	Advisory	Voting Proxy
	Ronald W. Pelletier	Advisory	Voting
	Nick Sturgeon	Voting	Advisory
	Kevin Mabry	Advisory	Advisory
	David Neel	Advisory	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Each of our sector sub-groups was tasked to create a whitepaper specific to their area. The goal of these papers is to identify organic cyber capabilities and capability gaps within Indiana to better inform decision makers allowing us to prioritize and apportion limited resources to support the needs of the state's critical infrastructure.
  - Since October, we have been working to capture and examine other state cyber response plans in an effort to identify the best of the best to assist the IECC in creating our own plan. To date, we have reviewed and uploaded to Syncplicity 15 of the best state plans.
  - Finally, we have been exploring "GRIDEX-like" exercise for both the water and election sectors.

- **Research Findings**
  - Based on initial findings from our research, we see the need to look not only at the Energy sector but also into other sectors especially water and waste-water treatment. The main effort of most plans appears to be Energy Sector centric, specifically targeting the Electric sub-sector. While an attack on this sector would be far reaching it is also a sector with much regulation, governance, established response protocols and exercise programs. We propose that the State also look at other sectors to exercise during the planning phase. Two that come to mind are the water/wastewater and State election systems. Unlike Energy, where the loss of power is seen immediately, the contamination of a water source, assisted by a cyberattack, could go undetected and have a far-reaching impact.
  - According to the Indiana Utility Regulatory Commission, there are 555 water utilities in the State of Indiana. The Environmental Protection Agency (EPA) estimates of $14 billion capital investments required over the next 20 years to update its aging infrastructure. These costs will directly compete with capital investment into cybersecurity. Penetration testing is not the total answer: In a Pre Incident environment and the thousands of organizations spread across all sectors within Indiana there is simply not enough capability in Department of Homeland Security (DHS), National Guard or the Private sector to accommodate even a fraction of the need. Our efforts would be better served on "teaching them to fish" - outreach and training thru sector exercises is a better use of these limited resources and farther reaching than a penetration assessment alone.
  - We would recommend that the IECC also look strongly at developing outreach, training, and exercises for other Sectors.

- **Working Group Deliverables**
  - Exercise
  - Cyber Emergency Response Team (IN-CERT)
  - Gap Analysis
  - Penetration Testing

- **Additional Notes "Measures of Success Over Time:"**
    - One Year: Teams trained and available to conduct professional vulnerability assessments. Concepts developed to support outreach, training and exercises in various sectors.
    - Three Years: Established Cyber exercises in sectors other than Energy. For example; a water treatment tabletop at the Muscatatuck Urban Training Center using both virtual and physical plant to demonstrate vulnerabilities and train sector workforce. Considering an election system tabletop.
    - Five Years: Nationally recognized leader in critical infrastructure cyber defense preparedness, training, exercises and response.

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. As these questions are more geared towards specific Critical Infrastructure, we will discuss emergency response capabilities and how the National Guard can play a supporting role in support to cyber emergency response for the state. Over the past five years, there have been several exercises and table tops, GRIDEx and Crit-Ex to mention a few. Their focus was less of a whole of Government approach and more focused on a single critical infrastructures response needs. In any large-scale cyber incident, multiple agencies (DHS, IDHS, Indiana State Police (ISP), Federal Bureau of Investigation (FBI), etc.) will need to work together. Coordination over the past five years between these agencies and the National Guard was limited. To operate effectively in cyberspace, these agencies will require strong relationships and practiced coordination to ensure and effective response. Our goal going forward is to ensure we build strong partnerships.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. The private sector owns and operates a vast majority of the nation's critical infrastructure; therefore, partnerships between State agencies in public and private sectors are essential to maintaining critical infrastructure, cybersecurity, and cyber resilience.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Practiced partnerships among State and Federal Cyber response agencies.

4. **What federal, state, or local cyber regulations is your area beholden to currently**?
    a. The National Guard can operate in three distinct statuses with different authorities. Each status impacts when and how the National Guard can respond to cyberspace events.
    b. The first status is fully federalized. This is governed by Title 10, U.S. Code. In this status, the National Guard is the same as the Active Duty Army or Air Force. The authorities and policies governing this status are beyond the scope of this questionnaire.

c. The second status is federally funded, but state-controlled. This is Title 32 Status and is normally used to provide training for the federal mission. This is the one weekend a month, two weeks in the summer status that is typically associated with the National Guard. Current authorities restrict both the type and scope of cyberspace operations that the National Guard can perform under Title 32. The primary policies governing this area include Dep Sec Def Memo 16-002, known as the "CTAA Memo", and DTM 17-007, referred to as the "Cyber DSCA Memo." These policies limit any actions to Defensive Cyberspace Operations/Internal Defensive Measures (DCO/IDM). The policies allow for coordination and consultation, but do not allow the National Guard to be used in a Title 32 status off Department of Defense Networks (DODIN), absent specific circumstances. Additional authorities govern what and how information is stored and/or processed by the National Guard under Title 32. These include the Freedom of Information Act (FOIA), the Privacy Act, and the Health Insurance Portability and Accountability Act (HIPAA).
d. Finally, the National Guard may operate in State Active Duty. This is both State funded and controlled. In this status, National Guardsmen operate as if they were agents of the State. While the personnel are governed purely by state law in this status, any federal equipment they use still has restrictions attached. Additional restrictions, such as licensing agreements to restrict which systems and programs may be used in State Active Duty or off Department of Defense Networks. The use of federal intelligence equipment, systems, and personnel are limited to SECRET and below under the CTAA memo. The National Guard is also governed by state laws in the area, such as data breach disclosure laws, state privacy laws and state information disclosure laws.
e. In both Title 32 and State Active Duty status, there is no authority to perform any yes no actions other DCO/IDM. Any other actions, such as offensive actions or defensive response actions would potentially submit a guardsman to liability under federal criminal laws. These include the Computer Fraud and Abuse Act, 18 U.S.C. §1030 et seq.; the Wiretap Act, 18 U.S.C. §2511 et seq.; the Pen Trap/Trace Act 18 U.S.C. §3121 et seq.; and the Stored Communications Act 18 U.S.C. §2701 et seq.
f. In summary, under Title 32, the National Guard is limited to coordination and consultation, absent specific exceptions. When activated by the Governor under state active duty the National Guard can respond to cyberspace incidents but is still limited in what federal equipment and systems they may use or access. As with the civilian sector, certain actions, such as offensive cyberspace operations and defensive response actions are prohibited and may subject the individual to criminal penalties.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Other state plans and DHS sector papers.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. Other state plans have been collected by this working group and posted to the Syncplicity portal site.

b. To help better inform our decision-making process, white papers are being developed by our sub-groups on where best to focus assessments with the limited resources available. These documents will be uploaded to the Syncplicity portal when completed.
c. This information will culminate in an Executive summary of the State of Indiana Critical Infrastructure Cyber Preparedness and a Critical Infrastructure Priority Matrix that will drive our cyber focus in the years to come.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
   a. See state plans uploaded to Synplicity.

8. **What does success look like for your area in one year, three years, and five years?**
   a. One Year: Teams trained and available to conduct professional vulnerability assessments. Concepts developed to exercise various sectors developed.
   b. Three Years: Established Cyber exercises in sectors other than electric. For example: a Water Treatment tabletop at the Muscatatuck Urban Training Center using both virtual and physical plant to demonstrate vulnerabilities and train sector workforce. Considering an election system tabletop.
   c. Five Years: Nationally recognized leader in critical infrastructure cyber defense preparedness, training and exercises.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
   a. N/A

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. N/A

11. **What do we need to do to attract cyber companies to Indiana**?
    a. We think the question is how do we build a culture within Indiana that emphasizes the importance of investing in cybersecurity? Many smaller entities must balance capital investments into infrastructure versus cyber defense capabilities. A public information campaign and targeted outreach is one method to consider. Demonstrating vulnerabilities is another under consideration within the Pre thru Post Cyber Working Group.

12. **What are your communication protocols in a cyber emergency?**
    a. These are currently being developed to support other sector plans.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. Best practices are well established across the sectors. As stated earlier in the document we need to develop the cyber culture through state and sector sponsored outreach.

Deliverable: Exercise

Deliverable: Exercise

General Information

1. **What is the deliverable?**
    a. Cross Sector Critical Infrastructure Exercise that highlights critical deficiencies in the targeted sector(s) and exercise State emergency response.

2. **What is the status of this deliverable?**
    a. The completion of the Executive summary of the State of Indiana Critical Infrastructure Cyber Preparedness and a Critical Infrastructure Priority Matrix will be used to focus a State Exercise. This deliverable is currently at less than 5% pending the completion of the aforementioned documents.

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Improved awareness and cyber health of the targeted sector(s).
    b. Emergency response processes validated.

6. **What metric or measurement will be used to define success?**
    a. Exercise conducted.

7. **What year will the deliverable be completed?**
    a. 2020

8. **Who or what entities will benefit from the deliverable?**
    a. Critical Infrastructure, State Government agencies and Local governments

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This type of service is also provided by Indiana Department of Homeland Security (IDHS), Indiana Office of Technology (IOT), and Indiana State Police (ISP).

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Lesson learned may be shared with the public awareness and training working group to assist in focusing outreach efforts.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IDHS, IOT, ISP.

12. **Who should be main lead of this deliverable?**
    a. Pre thru Post Working Group & IDHS

13. **What are the expected challenges to completing this deliverable?**
    a. Funding - The state will have to work the funding if required.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
[No Response]				

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes
b. **If Yes, please complete the following**:
   i. Unknown at this time, not counting Pre thru Post Working Group members.

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
Unknown at this time	Unknown at this time				

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.) Estimates only, nothing firm being too early in the process.

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Contractor	Run Exercise if large scale	$80,000[1]				

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Strengthen best practices to protect high risk Critical Infrastructure and improved coordination with interagency response with State Emergency Response Operations.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Improved awareness and cybersecurity posture.

19. What is the risk or cost of not completing this deliverable?

a. Continued risk and poor security posture.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. There is no measurable baseline. Success will be measured using After Actions Comments.

[1] This amount is rough order of magnitude and only used to identify potential costs. Once planning is initiated details of costs will be refined.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. **If Yes, please list states/jurisdictions**
    c. Many states do have a central hub for its cybersecurity efforts as outlined in their State Cybersecurity Plans collected and posted for the IECC members in Syncplicity portal.
    d. Based on the direction this working group takes we will then draw about this information to build metrics.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. Some states are still in a drafting state for Cybersecurity Plans.
    ii. Based on the direction this working group takes we will then draw about this information to build metrics.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Lack of cooperation among agencies and availability of state funding.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Currently this deliverable is designed as a one-time deliverable, therefore long-term design & support must be developed.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. We are currently researching and developing initial concept; therefore, no outreach has been conducted regarding implementation at this time.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Unknown at this time.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Unknown at this time.

Evaluation Methodology

Objective 1: The State of Indiana will develop and execute a Cross Sector Critical Infrastructure Cyber Exercise by December 2020.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Emergency Response Team (IN-CERT)

Deliverable: Cyber Emergency Response Team (IN-CERT)

General Information

1. **What is the deliverable?**
   a. Cyber Taskforce Enforcement Training

2. **What is the status of this deliverable?**
   a. Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. To provide a training program for Indiana law enforcement who will also be a part of a state cyber taskforce that is able to respond to large-scale cyber emergencies.

6. **What metric or measurement will be used to define success?**
   a. Set up of training and with 20 number of law enforcement signing up for the training.

7. **What year will the deliverable be completed?**
   a. When funding is secured

8. **Who or what entities will benefit from the deliverable?**
   a. Law enforcement, public and private entities

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Government Services

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. ISP, IDHS, and National Guard

12. **Who should be main lead of this deliverable?**
    a. ISP/IDHS

13. **What are the expected challenges to completing this deliverable?**
    a. Funding and establishing the new program.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Identify and price training	Group	100%	May 31	
Identify and price equipment	Group	100%	May 31	
Procure funding	Council Partners	0	TBD	
Identify personnel	Group	0	After funding procured	ISP to take lead
Begin training	Group	0	Within 12 months of funding procured	ISP to take lead

Resources and Budget

15. **Will staff be required to complete this deliverable?**
    a. No
    b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Training and certifications	KSAs to respond to cyber emergency. Certifications needed to provide skilled fact and expert testimony.	$556,060.00	$100,000/year	grants		
Forensic tools	Needed for cyber emergency response	$100,672.20	$75,000/year	grants		

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. A rapid, forensically sound response to cyber emergency.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Intercept commerce or public utility interruptions.

19. What is the risk or cost of not completing this deliverable?

a. Commerce and public utility interruptions. Failure to respond to cyber emergencies in a forensically sound manner and contamination of evidence such that bad actor attribution can't be accomplished.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Rapid response to cyber emergencies in a manner in which the response follows adopted norms and protocols, while being done in a forensically sound manner and ensuring preservation of evidence.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?
training availability

a. Inability to obtain grant funding.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Continue funding along with continued training.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Chetrice Mosley

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. Any State law enforcement agency during the course of cybercrime investigations. Also provides a response to State prosecutors and courts for skilled fact and expert witnesses.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. ISP, IDHS, and Indiana National Guard (INNG)

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No

30. What are other public relations and/or marketing considerations to be noted?

a. None at this time.

Evaluation Methodology

Objective 1: Indiana State Police will develop and launch Indiana Cyber Emergency Response Team training program within 12 months of the Council partners securing an encumbered source of funding.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Gap Analysis

Deliverable: Gap Analysis

General Information

1. **What is the deliverable?**
   a. Gap Analysis – the identification of unfilled requirements within the state that presents a risk to cybersecurity.

2. **What is the status of this deliverable?**
   a. This requirement is on-going and has no start or end.

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☒ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Better aligned limited resources to high risk.

6. **What metric or measurement will be used to define success?**
   a. Our ability as a state to identify and then fund and fill critical gaps. This effort will not stop as it must be continually evaluated to identify new risks and gaps that need addressing.

7. **What year will the deliverable be completed?**
   a. This line of effort is on-going and has no definitive end date.

8. **Who or what entities will benefit from the deliverable?**
   a. Critical Infrastructure, State Government agencies and Local governments

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This type of service is also provided by IDHS, IOT, ISP.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. As gaps are identified and evaluated, other groups will be brought into the process.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. This depends on the gap being considered. In many cases IDHS, IOT, and/or ISP.

12. **Who should be main lead of this deliverable?**
    a. Pre thru Post Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Funding - The state will have to work the funding.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability**?
    a. It's a sustained effort because gaps must be continually identified. Each gap identified is a one-time deliverable to remediate it.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
N/A				

Resources and Budget

15. **Will staff be required to complete this deliverable?**
    a. Yes
    b. **If Yes, please complete the following**
        i. Unknown at this time.

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. Unknown at this time.

Resource	Justification/ Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Risks are mitigated.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Costs and risk are evaluated for each identified gap and handled under separate documentation.

19. What is the risk or cost of not completing this deliverable?

a. Identified the risks that are not mitigated.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success and metrics are evaluated for each identified gap and handled under separate documentation.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Unknown at this time

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Unknown at this time

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Unknown at this time

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. N/A

27. Can this deliverable be used by other sectors?

a. N/A, each identified gap is handled under separate documentation.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Dependent on each gap identified.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Potentially

30. What are other public relations and/or marketing considerations to be noted?

a. Unknown at this time.

Evaluation Methodology

Objective 1: IECC Cyber Pre thru Post Incident Working Group will complete a comprehensive gap analysis of identified high risk critical infrastructure sectors by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Cyber Pre thru Post Incident Working Group provide recommendations based on a comprehensive gap analysis of identified high risk critical infrastructure sectors by December 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☒ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Assessments

Deliverable: Cyber Assessments

General Information

1. **What is the deliverable?**
    a. Cyber assessments will be developed and delivered along two distinct lines: 1) Developing partnerships to support and augment local/state government entities cyber assessment requirements. 2) Developing baseline risks for an identified Indiana critical infrastructure structure to inform a cyber exercise.

2. **What is the status of this deliverable?**
    a. In-progress; 25% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Independent assessment of network vulnerabilities.

6. **What metric or measurement will be used to define success?**
    a. Ability to sustain 2 tests per month.

7. **What year will the deliverable be completed?**
    a. To start no later than (NLT) Dec 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Initially state government agencies and then local governments

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This type of service is also provided by DHS.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Lesson learned may be shared, without identification of agency, with the public awareness and training working group to assist in focusing outreach efforts.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IDHS

12. **Who should be main lead of this deliverable?**
    a. Pre thru Post Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Funding - State active duty fund will be required in order for Nation Guard personnel to work on non-Department of Defense (DoD) networks.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop Concept	INNG	25%	TBD	Personnel are mobilized and will not be available until late summer 2018 to start developing this program.

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

i. Costs are based on two weeks (ten days) with four personnel per day.

Assessment Costs: (personnel)
1 - O4 Cyber Team Chief
1 - W3 Cyber Tech lead
1 - E8 Cyber Operators
1 - E7 Cyber Operators

Assessment/PEN Costs						
		day		*week*		*month*
a. Pay	$	898.40	$	4,491.99	$	19,315.56
b. BAH	$	74.70	$	373.50	$	1,606.05
c. Lodging and Rations	$	162.00	$	810.00	$	3,483.00
d. BAS	$	41.46	$	207.31	$	891.42
GRAND TOTAL	**$**	**1,176.56**	**$**	**5,882.80**	**$**	**25,296.03**

Time Line: (typically two weeks for a basic assessment or penetration (PEN) test of a medium to small organization.
- Five days (collection of assets and resources information, objectives identified)
- 2-3 days (Hands-on assessment PEN testing)
- 2-3 days (Findings report publish and reviewed with the customer, best practices provided)

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
see above		Cyber CPT	State Active Duty	none	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Non DoD equipment	Use of Federal funding maybe disallowed	$40,000	$5,000	State	none	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Under current definitions of U.S. Title 10 law and Department of Defense Directives the use of federally funded equipment for the National Guard could be utilized to support the Governor only by those Service Members while serving in a "State Active Duty" status. Any cyber response team, existing of non-military members, would require equipment procured outside of Federal channels, e.g. State or self-funded. Estimates in the table above are the rough order of magnitude costs to the State if the purchase of basic cyber assessment equipment sets were required.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Not measurable

19. What is the risk or cost of not completing this deliverable?

a. Status quo, no improvement in cyber readiness.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success will be measured by executing one (1) assessment per month starting 2019 and dependent on the State providing funding.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. If Yes, please list states/jurisdictions
    i. Ohio, Washington, Virginia

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Willingness of State agencies or Critical Infrastructure Sector to allow assessments. Lack of state funding.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. To truly sustain this for the state would require fulltime personnel as National Guard soldiers must take leave from their full-time jobs to conduct these tests. We have no full-time personnel on staff.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. [No Response]

27. Can this deliverable be used by other sectors?

a. [No Response]
b. **If Yes, please list sectors**
    i. N/A

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. On-going

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Unknown at this time.

Evaluation Methodology

Objective 1: Indiana National Guard will develop a Local/State Government Cyber Assessment Program by December 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indiana National Guard will conduct Cyber Assessment for State critical infrastructure entities by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

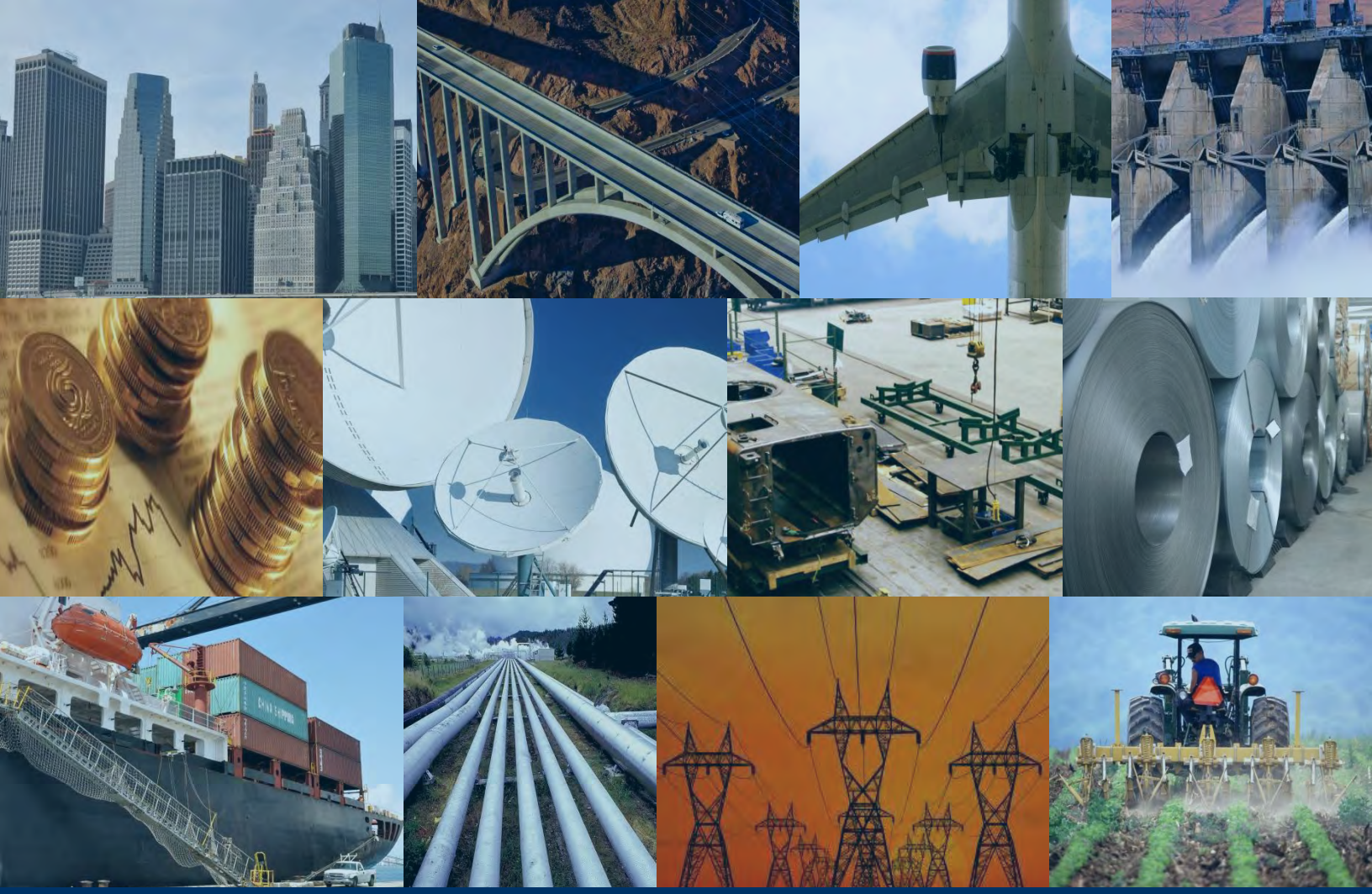
This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Department of Homeland Security (DHS) Sector Risk Snapshots
- IECC Cyber Vulnerabilities Whitepaper – Communications Sector
- IECC Cyber Vulnerabilities Whitepaper – Energy Sector
- IECC Cyber Vulnerabilities Whitepaper – Water and Wastewater Sector
- IECC Pre- through Post-Incident White Paper – Education Sector
- Indiana National Guard (INNG) State Cyber Baseline Survey Results

Department of Homeland Security (USDHS)

Sector Risk Snapshots

May 2014



Sector Risk Snapshots

May 2014

Homeland Security

Sector Risk Snapshots

Introduction

Ensuring the security and resilience of critical infrastructure—those assets, systems, and networks that underpin American society—is essential to the Nation's security, public health and safety, economic vitality, and way of life. Managing risks to critical infrastructure requires an integrated approach across the whole-of-community to:

- Identify, deter, detect, and prepare for threats and hazards to the Nation's critical infrastructure;
- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

Mission

Strengthen the security and resilience of the Nation's critical infrastructure by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure protection community.

National Infrastructure Protection Plan (NIPP), 2013

Presidential Policy Directive 21 (*PPD-21)* on *Critical Infrastructure Security and Resilience*, builds on the extensive work done to date to protect critical infrastructure, and identifies 16 critical infrastructure sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

This compendium of Sector Risk Snapshots provides a brief overview and risk profile of the 16 critical infrastructure sectors, the Education, Electric, and Oil and Natural Gas Subsectors, and the seven Transportation Systems Modes. The Snapshots provide an introduction to the diverse array of critical infrastructure sectors, touching on some of the key threats and hazards concerning the sectors, and highlighting the common, first-order dependencies and interdependencies between sectors. The Snapshots are intended to serve as quick reference aids for homeland security partners, particularly State and local partners, and fusion center analysts, and each Snapshot includes a list of resources that partners can go to for more comprehensive sector information.

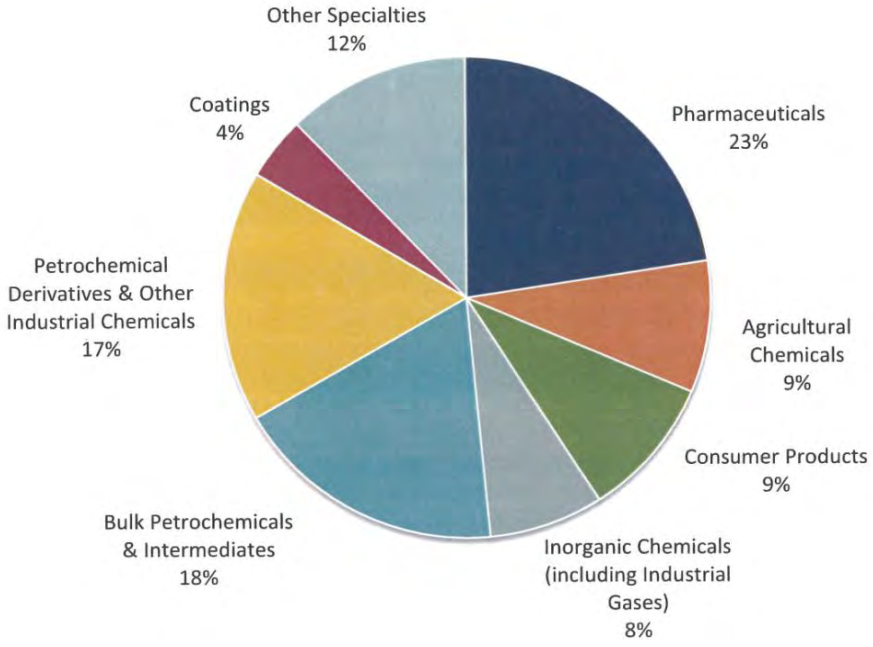
Prepared by the DHS Office of Cyber and Infrastructure Analysis (OCIA). For more information, contact OCIA at OCIA@hq.dhs.gov or visit our Website at www.dhs.gov/office-cyber-infrastructure-analysis.

Homeland Security

Chemical Sector Sector Risk Snapshot

Figure 1: Approximately 13,500 Chemical Manufacturing Facilities are in the U.S., owned by more than 9,000 Companies. *Source: Environmental Protection Agency (EPA, 2011)*

Figure 2: Global Chemical Shipments by Segment (as a percent of total shipments)



Chemical Sector Overview

- **The Chemical Sector is an integral component of the U.S. economy, employing nearly 1 million people, and earning annual revenues between $600 and $700 billion.**
- **Chemical Sector facilities typically belong to one or more of four key functional areas: (1) manufacturing plants, (2) transport systems, (3) warehousing and storage systems, and (4) chemical end users. In addition, companies may operate facilities across multiple functional areas, for example, a chemical manufacturer may also own a trucking and distribution operation.**
- **While the key functional areas primarily describe their physical characteristics and activities, each of the four functional areas depends on cybersystems for a variety of purposes, including operating manufacturing processes, tracking inventory, and storing customer information.**
- **As one of the oldest industries in the country, the chemical industry has a long history of resilience, based on the sector's ability to adapt to, prevent, prepare for, and recover from all hazards, including natural disasters, fluctuating markets, or a change in regulatory programs.**
- **To maintain operational resilience, successful businesses identify their critical dependencies and interdependencies and develop appropriate strategies to manage critical systems disruptions, should they occur.**
- **The DHS Chemical Facility Anti-Terrorism Standards (CFATS) program identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals. Upon review of more than 44,000 preliminary assessments from facilities with chemicals of interest, 4,275 facilities are now covered by CFATS (DHS, 2013).**

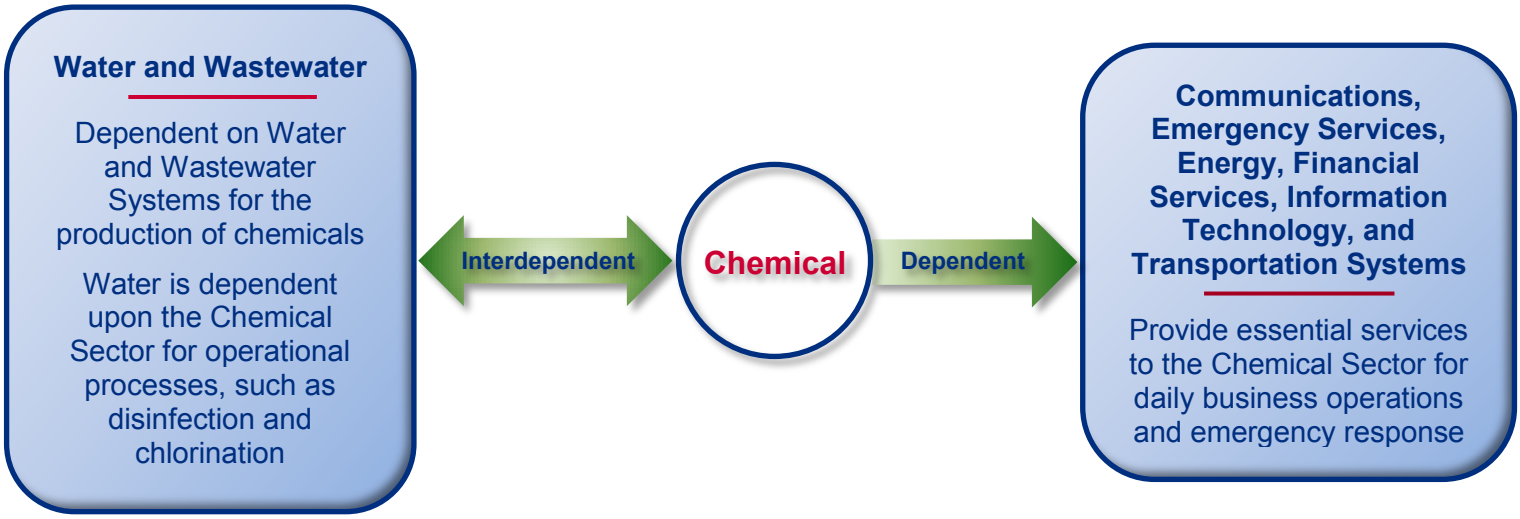
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - The Chemical Sector is vulnerable to the threat of malicious actors physically or remotely manipulating network-based systems designed to control chemical manufacturing processes or process safety systems.
  - The physical disruption inflicted upon industrial assets in 2010 by the Stuxnet worm is evidence that control systems are vulnerable to increasingly destructive attacks and that the U.S. critical infrastructure may face cyberattacks of increasing sophistication.
- **Insider Threat**
  - While a facility can increase its physical security measures substantially, insiders with access who choose to intentionally cause harm will continue to contribute risk to the Chemical Sector. (CFATS, 2010, www.federalregister.gov/articles/2010/04/13/2010-8312/national-protection-and-programs-directorate-chemical-facility-anti-terrorism-standards-personnel#h-10)
  - Factors that improve management of this risk include greater cooperation and less competition among owners and operators within the sector and relatively higher cooperation between owners and operators and their workforces. (NIAC, *Insider Threat*, 2008, www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf)
- **Natural Disasters and Accidents**
  - Natural disasters and accidents contribute to the ongoing risk of exposing the environment and the population to chemicals.
  - Accidents such as the 2013 West Fertilizer Company explosion—an ammonium nitrate explosion that resulted in 15 deaths, over 160 injuries, and more than 150 damaged or destroyed buildings in West, Texas—demonstrate the significant potential consequences of incidents involving harmful chemicals.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, chemicalsector@hq.dhs.gov and www.dhs.gov/chemical-sector
- DHS, *National Risk Pro*file, OCIA@hq.dhs.gov.
- National Infrastructure Protection Plan, www.dhs.gov/national-infrastructure-protection-plan
- Maritime Transportation Security Act of 2002, www.tsa.gov/assets/pdf/MTSA.pdf
- Chemical Facility Anti-Terrorism Standards (CFATS), www.dhs.gov/chemical-facility-anti-terrorism-standards

Figure 3: Common, First-order Dependencies and Interdependencies of the Chemical Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Commercial Facilities Sector
Sector Risk Snapshot

Critical Infrastructure Protection Issues

- Owners and operators are responsible for the day-to-day protection of commercial facilities, in close cooperation with local law enforcement.
- The Government has various programs and efforts to support the protection of commercial facilities. Activities include providing timely threat indications and warnings, and working with organizations to identify vulnerabilities and mitigate risks through protective programs and training.
- Given the national-level visibility and potential human and economic consequences of prominent commercial facilities, it is important for the Federal Government and the Commercial Facilities Sector to work together to ensure the protection of the Nation's prominent business centers and public gathering places.

The Department of Homeland Security oversees the implementation and execution of protective measures programs across the Commercial Facilities Sector. Some of the programs currently underway include:

Risk Self-Assessment Tool (RSAT): Delivers an all-hazard analysis of a facility's current risk level and offers options for consideration on reducing and managing potential vulnerabilities.

Protective Security Advisor (PSA) Program: PSAs are critical infrastructure protection and vulnerability assessment specialists with a wealth of anti-terrorism and security experience deployed across the U.S.

Bomb-making Materials Awareness Program (BMAP): Assist commercial retailers, commercial service providers, and chemical distributers/wholesalers in identifying suspicious purchases of materials used in home-made explosive or improvised explosive device manufacturing.

Protective Measures Guides: An overview of possible threats, vulnerabilities, and protective measures designed to assist facility owners and operators in planning and managing security specific to their venue to maintain a safer environment for guests and employees.

Suspicious Activity Videos: Designed to raise the level of awareness for hotel and retail employees by highlighting the indicators of suspicious activity.

Commercial Facilities Sector Overview

- **Commercial Facilities Sector operates on the principle of open public access, meaning that the general public can move freely throughout these facilities without the deterrent of highly visible security barriers.**
- **The majority of the facilities in this sector are privately owned and operated, with minimal interaction with the Federal Government and other regulatory entities.**
- **The Commercial Facilities Sector consists of the following eight subsectors:**

1. **Public Assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers);**
2. **Sports Leagues (e.g., professional sports leagues and federations);**
3. **Gaming (e.g., casinos);**
4. **Lodging (e.g., hotels, motels, conference centers);**
5. **Outdoor Events (e.g., theme and amusement parks, fairs, campgrounds, parades);**
6. **Entertainment and Media (e.g., motion picture studios, broadcast media);**
7. **Real Estate (e.g., office and apartment buildings, condominiums, mixed-use facilities, self-storage); and**
8. **Retail (e.g., retail centers and districts, shopping malls).**

Threats and Hazards of Significant Concern

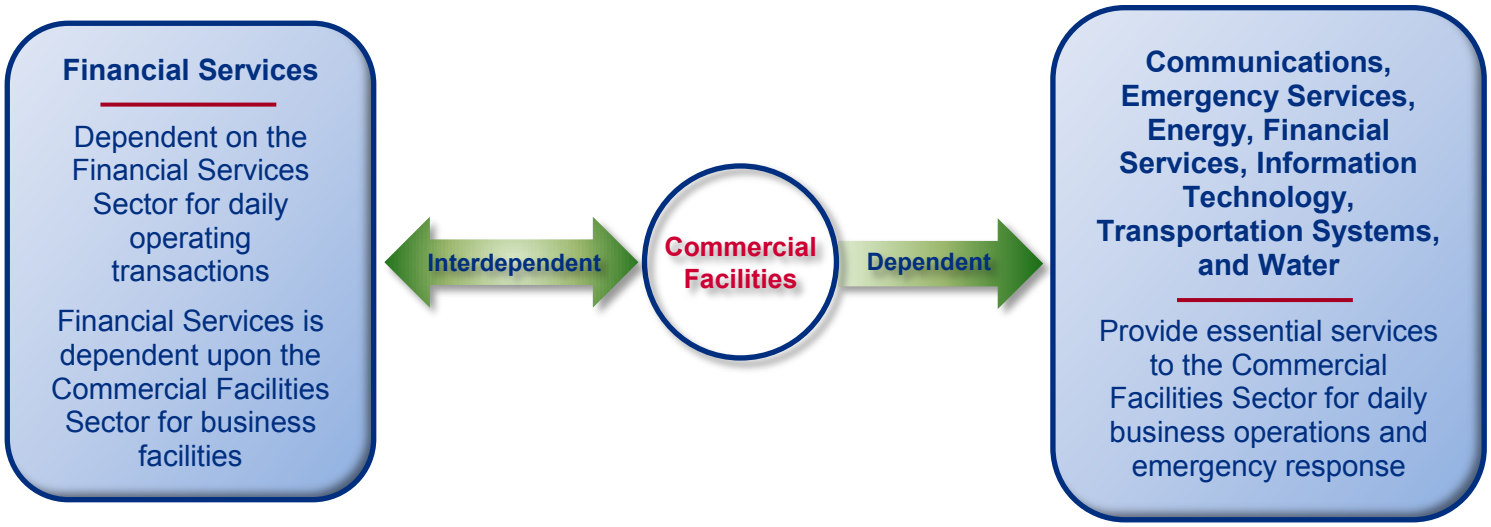
The Commercial Facilities Sector operates through a principle of open public access, which can increase the vulnerability to many types of attack methodologies. In addition, many Commercial Facilities Sector venues are highly recognizable, thus increasing the potential attractiveness to an adversary. These characteristics increase the risk to the Commercial Facilities Sector.

- **Bombings**
  - The adversary has expressed interest, and has a history of the use of explosive attacks against the Commercial Facilities Sector.
  - This attack methodology has the potential for creating mass casualties.
- **Active Shooter**
  - While a small arms attack may produce fewer casualties then an explosive attack, this attack methodology requires fewer resources and planning.
  - As in the case with bombings, the sector's open public access and population density make commercial facilities vulnerable to small arms attacks, resulting in an increased risk to the sector.
- **Chemical, Biological, Radiological (CBR) Attacks**
  - Some terrorist organizations have expressed interest in acquiring and using CBR weapons. Given the nature of mass gathering, and open public access of the Commercial Facilities Sector, there are unique vulnerabilities to either the distribution of CBR materials through ventilation systems or through liquid distribution in an open arena type environment.
  - Outdoor facilities, such as public assemblies or sporting events, are also at risk. Al-Qaeda has previously expressed interest in obtaining crop dusters, which could be used to disseminate aerosolized CBR agents over large areas and gatherings.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/commercial-facilities-sector
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov.
- Commercial Facilities Resources: www.dhs.gov/commercial-facilities-resources

Figure 1: Common, First-order Dependencies and Interdependencies of the Commercial Facilities Sector



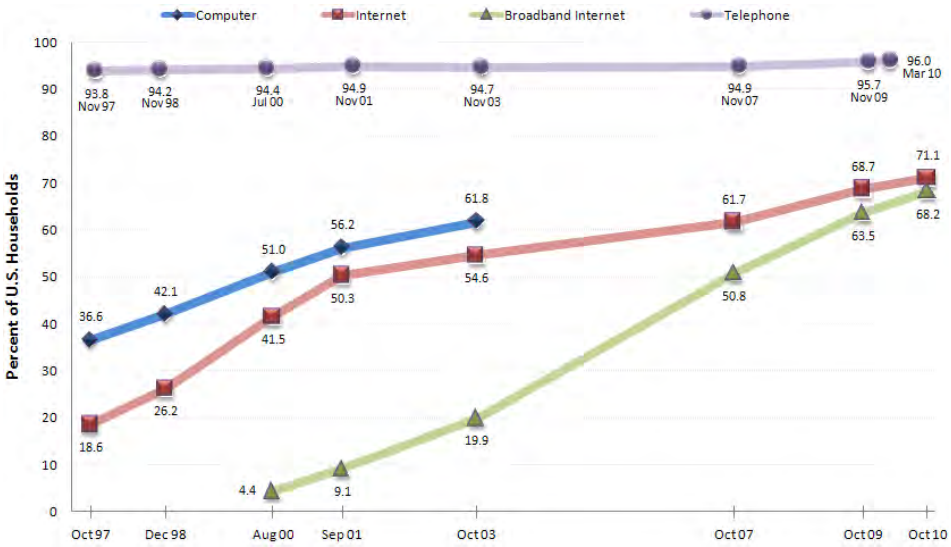
May 2014

Homeland Security
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Communications Sector
Sector Risk Snapshot

Figure 1: U.S. Households with Computers, Telephone Subscriptions, and Internet Access, Selected Years, 1997-2010



*Note: 2001-2012 use 2000 Census-based weights and earlier years use 1990 Census-based weights
Source: National Telecommunications and Information Administration, February 2011

Types of Communications Infrastructure

- **Wireline Communications**: Consists primarily of the public switched telephone network (PSTN) and includes cable networks and enterprise networks. Wireline networks also are being redefined by next generation networks (NGNs), which are high-speed, converged circuit-switched and packet-switched networks capable of transporting and routing a multitude of services, including voice, data, video, and other multimedia, across various platforms. The wireline component also includes the Internet infrastructure and submarine cable infrastructure.
- **Wireless Communications:** Consists primarily of cellular telephone, paging, personal communications services, high-frequency radio, unlicensed wireless, and other commercial and private radio services, including numerous law enforcement, public safety, and land mobile radio systems.
- **Satellite Communications:** Satellite communications systems deliver data, voice, and video services. Networks may be private and independent of the terrestrial infrastructure or may share common facilities (e.g., a teleport) and be combined with terrestrial services to deliver information to the intended recipient(s). Important satellite network components include ground stations; telemetry, tracking, and command links (TT&Cs); very small aperture terminals (VSATs); and data links.
- **Cable:** Cable communications systems are wireline networks that offer analog and digital video programming services, digital telephone service, and high-speed Internet access service. Cable systems use a mixture of fiber and coaxial cable that provide two-way signal paths to the customer.
- **Broadcasting:** Broadcasting systems consist of free, over-the-air radio and television stations that offer analog and digital audio and video programming services and data services.

Communications Sector Overview

- **The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Over the last 25 years, the Sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry, using terrestrial, satellite, and wireless transmission systems.**
- **The transmission of these services has become very interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic, and companies routinely share facilities and technology to ensure interoperability and efficiency.**
- **The private sector, as owners and operators of the majority of communications infrastructure, is the primary entity responsible for protecting Sector infrastructure and assets.**
- **Working with the Federal Government, the private sector is able to predict, anticipate, and respond to Sector outages and understand how they might affect the ability of the national leadership to communicate during times of crisis, impact the operations of other Sectors, and affect response and recovery efforts.**
- **The Communications Sector is closely linked to a number of other Sectors, including Energy, Information Technology, Financial Services, Emergency Services, and Postal and Shipping.**

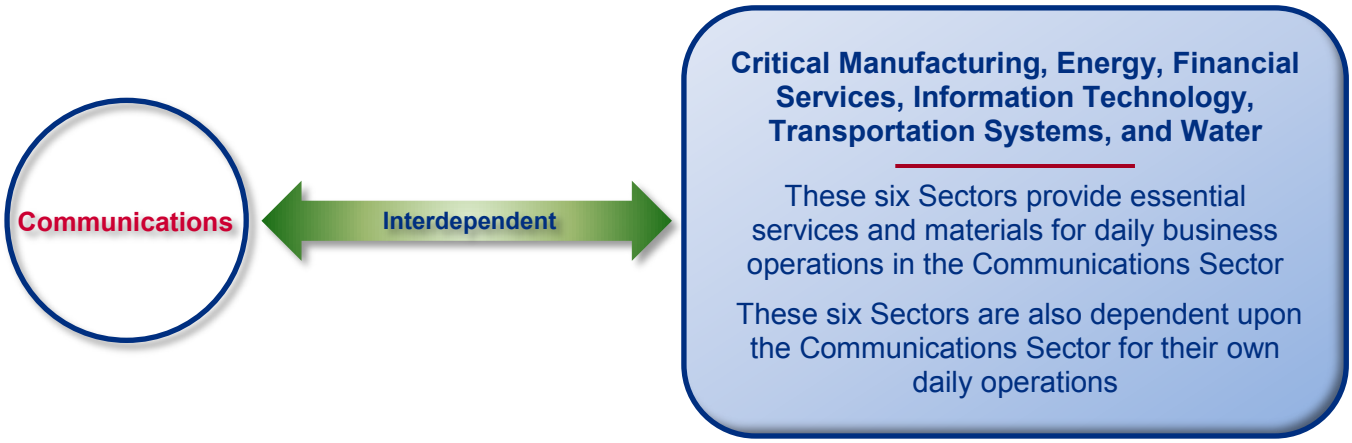
Threats and Hazards of Significant Concern

- **Single physical incidents**, such as nuclear detonations, major earthquakes, hurricanes, and space weather are likely to significantly disrupt the Sector over large regions. The Sector hardens systems and applies the principle of diversity (employing various primary and alternative routing and systems) and the principle of redundancy (using backup or multiple capabilities to sustain operations) to mitigate these and other threats (e.g., those that could cause potential damage to underground infrastructure from digging).
  - Space weather, such as severe solar geomagnetic storms, can cause high-power transformers to fail and electrical systems to possibly collapse. Because of the dependence of communications systems on electrical power, communications networks would soon fail in the event of a long-term, large-scale electrical network collapse. Solar weather can also directly degrade communications satellites and disrupt global positioning system (GPS) functionality (interfering with GPS satellites and their signals). Short-term loss or disruption of GPS will have minimal impacts on the underlying infrastructure, but medium- to long-term loss will degrade GPS-reliant services provided through the wireless, satellite, cable, and broadcast networks.
- **Cyber-disruptions** of communications systems present unique challenges due to global connectivity. The exploitation of vulnerabilities halfway around the world can begin affecting critical U.S. communications components in a matter of minutes.
- **Malicious actors** pose one of many human risks, which can impact data, networks, and components, as well as create financial losses for organizations.
  - The use of high-altitude electromagnetic pulse (EMP) weapons, source region EMP weapons, intentional electromagnetic interference devices, and high-energy radio frequency weapons could damage both electrical and communications systems.
  - Breached supply chain integrity could also result in disruption of service and network availability, loss of network control, loss of confidentiality and integrity of communications, unauthorized access, and disruption of emergency telecommunications, as well as fraud and theft of service.

For More Information

- Sector-Specific Agency: DHS, Office of Cybersecurity and Communications, www.dhs.gov/office-cybersecurity-and-communications
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/communications-sector

Figure 2: Common, First-order Interdependencies of the Communications Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Critical Manufacturing Sector
Sector Risk Snapshot

Figure 1: Manufacturing's Role in the U.S. Economy

* Exports data from 2010. R&D Data from 2009, the last available. All other data from 2011.
Source: U.S. Department of the Treasury

Several characteristics of today's manufacturing environment are common across each of the key functional areas within the Critical Manufacturing Sector. Examples include the following:

1. **Most manufacturing enterprises are integrated into complex, interdependent supply chains.** Few businesses operate independently. Nearly all manufacturers are part of a chain of suppliers, vendors, partners, integrators, contractors, and customers that link to other industries and businesses.
2. **Supply chains have been optimized for productivity and efficiency.** Competitive pressures cause businesses to optimize their manufacturing processes through highly coordinated business arrangements that enable manufacturers to maintain low inventories of raw materials and intermediate and end products.
3. **Manufacturers have become highly reliant on global information and communication systems.** Automation, control, information, processing, robotics, telecommunications, and the Internet have radically improved industrial productivity and have reshaped the operations and asset base of manufacturers.
4. **Globalization and outsourcing have linked U.S. manufacturers with foreign suppliers, vendors, and customers through highly interdependent supply networks.** Manufacturers have increasingly turned to foreign markets for raw materials, component manufacturing, equipment and machinery, labor, and customers as a way to reduce overall costs.
5. **Manufacturers rely heavily on energy sources for heat, power, and raw materials.** While all businesses are dependent on energy, manufacturers typically require large amounts of these resources, much of it in the form of hard-to-store electricity and natural gas.

Critical Manufacturing Sector Overview

- **The Critical Manufacturing Sector is crucial to the economic prosperity and continuity of the United States. Products designed, produced, and distributed by U.S. manufacturers make up 12 percent of the U.S. gross domestic product and directly employ nearly 12 million of the Nation's workforce.**
- **The Critical Manufacturing Sector identified the following industries to serve as the core of the Sector:**
  - **Primary Metal Manufacturing**
  - **Machinery Manufacturing**
  - **Electrical Equipment, Appliance, and Component Manufacturing**
  - **Transportation Equipment Manufacturing**
- **These key functional areas depend upon physical, cyber, and human elements to perform their missions:**
  - **Physical elements include the facilities supporting each functional area.**
  - **Human elements include the personnel associated with each function.**
  - **The cyber-elements include electronic systems for processing the information necessary for management and operation or for automatic control of physical processes.**
- **Each key functional area has unique markets, assets, business models, and competitive conditions that shape the critical manufacturing risk profile.**
- **Products made by these manufacturing industries are essential in varying capacities to many other critical infrastructure sectors.**

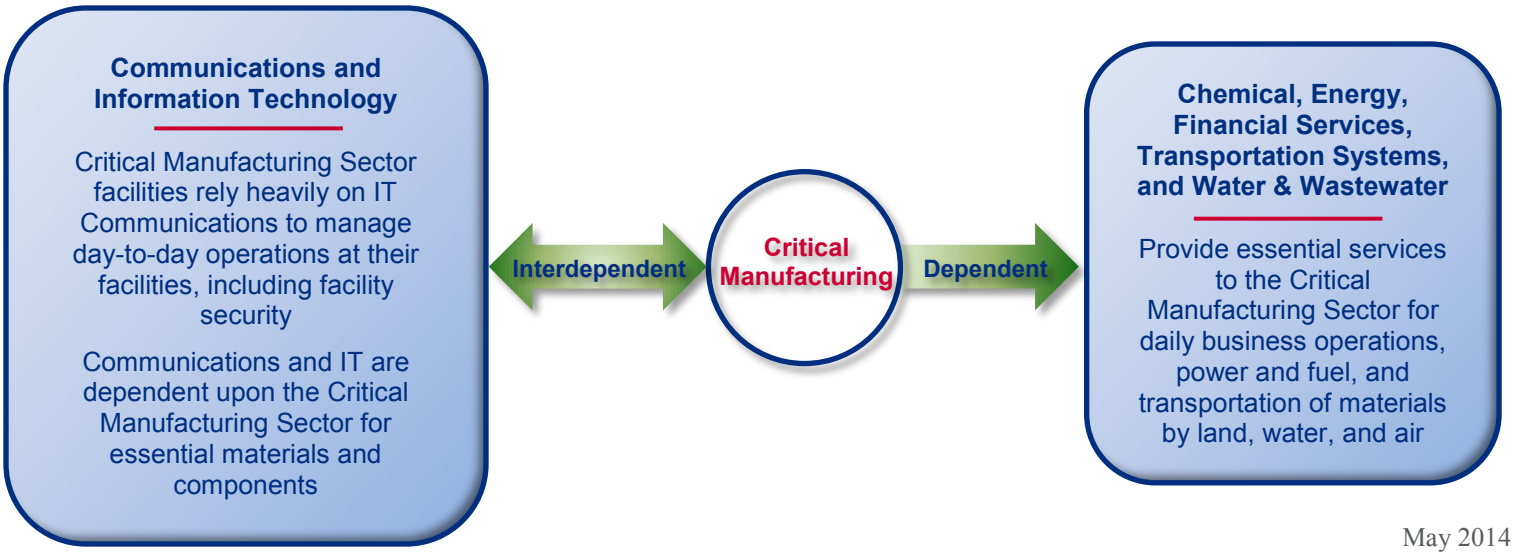
Threats and Hazards of Significant Concern

- **Supply Chain Vulnerability**
  - Supply chains at key inbound transportation nodes are of particular concern because incidents are likely at nodes, such as domestic ports. There is also a potential for large-scale consequences to the many industries that rely on the importation of materials and products.
  - Lean inventory and just-in-time practices, as well as greater distances from components or raw materials required for production to the delivery of finished products to markets, have made the Critical Manufacturing Sector more sensitive to transportation disruptions and fuel costs.
  - Supply chain systems are also more vulnerable because fewer basic metals and minerals are mined and processed in the United States, thereby increasing our dependence on foreign countries to provide these materials.
- **Cyberthreats**
  - Unauthorized on-site or remote intrusion into sector industrial control systems and supervisory control and data acquisition systems poses a growing threat and contributes to risk for the Critical Manufacturing Sector.
  - Supply chain systems are more vulnerable because of increased reliance on advanced information technology (IT) systems. Critical infrastructure owners and operators are also slow to adopt security and risk management measures for systems. Nation-states and other actors could potentially defeat competition and/or obtain competitive secrets through cyberintrusion.
- **Insider Threat**
  - The sector's systems are complex and increasingly dependent on information technology, making the sector highly susceptible to exploitation by current and former industry employees and contractors with malicious intent and unique knowledge of, and access to, these systems.
  - Threats posed by malicious insiders may include sabotage, theft or diversion, cyberattacks, or terrorism against critical manufacturing facilities.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/about-office-infrastructure-protection
- DHS, Sector Specific Profile: www.dhs.gov/critical-manufacturing-sector-critical-infrastructure
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies and Interdependencies of the Critical Manufacturing Sector



May 2014

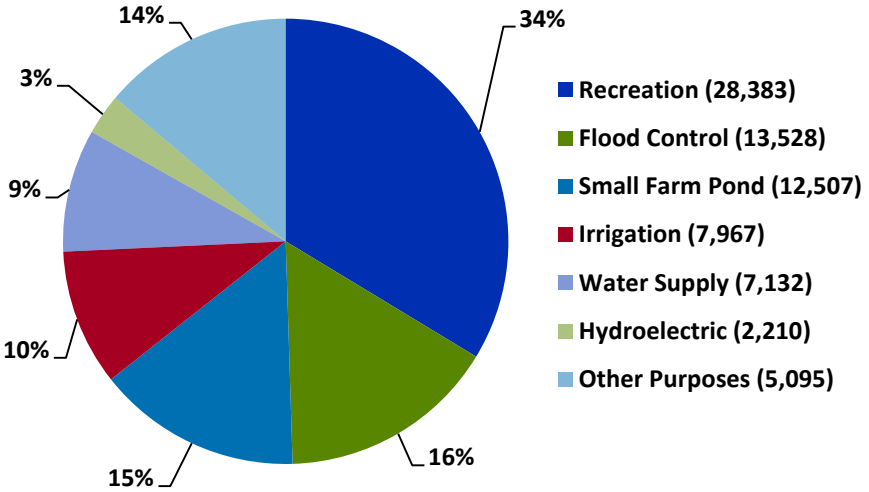
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Dams Sector Sector Risk Snapshot

Figure 1: Primary Purpose or Benefit of U.S. Dams



Dams Sector assets are vital components of the Nation's infrastructure. Some examples of the benefits derived from sector assets are:

Water Storage and Irrigation: Dams create reservoirs that supply water for a multitude of industrial, municipal, agricultural, and recreational uses throughout the United States.

Electricity Generation: Dams in the United States produce more than 270,000 gigawatt-hours of the Nation's electricity, representing 70 percent of the Nation's renewable energy generation, and over 6 percent of U.S. electricity generation overall.

"Black Start" Capabilities: There are 4,316 megawatts of "incremental" hydropower available at sites with existing hydroelectric facilities. Incremental is defined as capacity additions or improved efficiency at existing hydro projects.

Recreation: Dams and other sector assets provide prime recreational facilities throughout the United States.

Navigation: The U.S. waterway system, which includes 236 lock chambers at 192 lock sites owned and/or operated by the U.S. Army Corps of Engineers (USACE).

Flood Risk Reduction: Many dams and levees function as flood control projects, thereby reducing the potential human health and economic impacts of flooding.

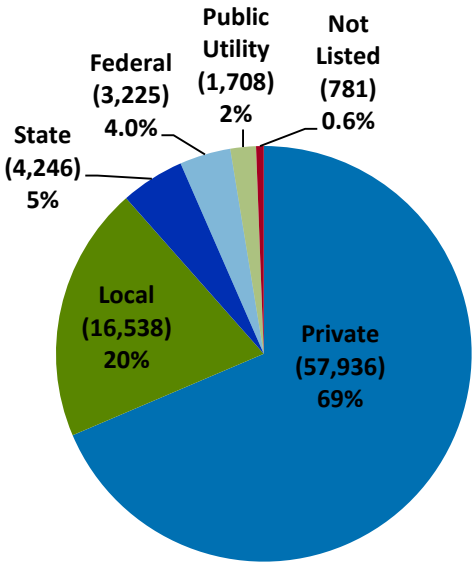
Sediment Control: Some dams enhance environmental protection by controlling detrimental sedimentation.

Impoundment of Mine Tailings and Industrial Waste Materials: More than 1,500 mine tailings and industrial waste impoundments controlled by dams in the Nation facilitate mining and processing of coal and other vital minerals.

Dams Sector Overview

- The Dams Sector comprises assets that include dam projects, hydropower generation facilities, navigation locks, levees, dikes, hurricane barriers, mine tailings, industrial waste impoundments, and other similar water retention and water control facilities.
- The Dams Sector is a vital and beneficial part of the Nation's infrastructure. It continuously provides a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation.
- There are more than 84,000 dams in the United States; approximately 69 percent are privately owned, and more than 85 percent are regulated by State dam safety offices.

Figure 2: Dam Ownership in the U.S.



Source Figures 1-2: DHS, Dams Sector-Specific Plan, *2010, www.dhs.gov/dams-sector.*

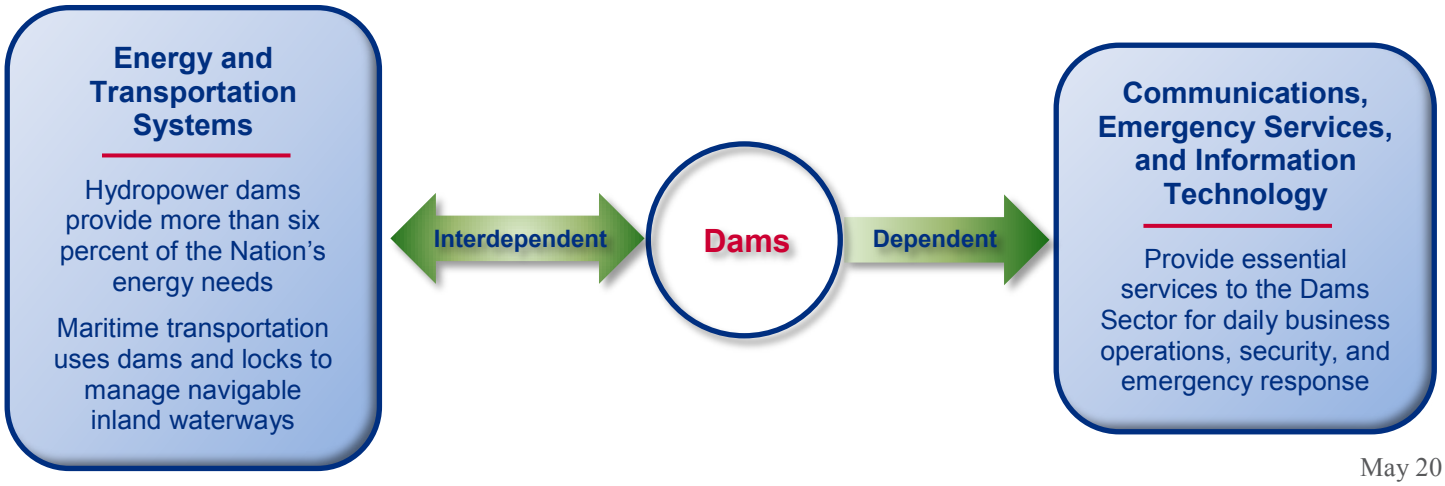
Threats and Hazards of Significant Concern

- **Natural Hazards**
  - Extreme flooding and severe storm surges can overwhelm the flood storage capacity of reservoirs and levee systems and lead to breaching or overtopping.
  - The consequences of extreme levee failure were seen in the aftermath of Hurricanes Katrina and Rita in 2005, which resulted in the deaths of more than 1,800 people and more than $200 billion in economic damages.
  - Earthquake ground motion may also lead to severe damage or failure, as evidenced by the failure of Fujinuma Dam in Japan following the Tōhoku earthquake in March 2011.
- **Malicious Actors**
  - With the necessary capabilities and resources, adversaries could potentially achieve catastrophic failure and severely disrupt missions through the use of improvised explosive devices (IEDs), increasing risk for the Sector.
  - Dams Sector assets have experienced at least 20 kinetic attacks worldwide over the last decade, and adversaries could exploit the inherent vulnerabilities of these public facilities (Source: National Consortium for the Study of Terrorism and Responses to Terrorism, Global Terrorism Database, 2011).
  - Adversaries could bypass land-based security measures with water-borne IEDs and strike dams, locks, or levees. Vehicle-borne IEDs (VBIEDs) could also reach the crest of dams or levees, particularly those with roads providing vehicular access. An assault team could overpower security forces, seize a facility's control room, and detonate IEDs, as occurred in a July 2010 attack against a Russian hydropower station.
  - The increasing use of standardized industrial control systems (ICS) technology increases the sector's potential vulnerability to direct cyberattacks and intrusions, which are a constant potential threat across the critical infrastructure community.
- **Aging Infrastructure**
  - Some dams, inland waterways, and levees are in increasingly poor condition as a result of aging, deterioration, and maintenance backlogs. This increases the risk to the Dams Sector, as its infrastructure continues to age.
  - The average age of the 84,000 dams in the country is 52 years old. The number of deficient dams is estimated at more than 4,000, which includes 2,000 deficient high-hazards dams. In addition, 91 percent of U.S. levees are not in acceptable condition (Source: American Society of Civil Engineers, *Infrastructure Report Card,* 2013).

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/dams-sector
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS, *Dams Sector: Roadmap to Secure Control Systems,*2010
- USACE, National Inventory of Dams, http://nid.usace.army.mil

Figure 3: Common, First-order Dependencies and Interdependencies of the Dams Sector



May 2014

Homeland Security

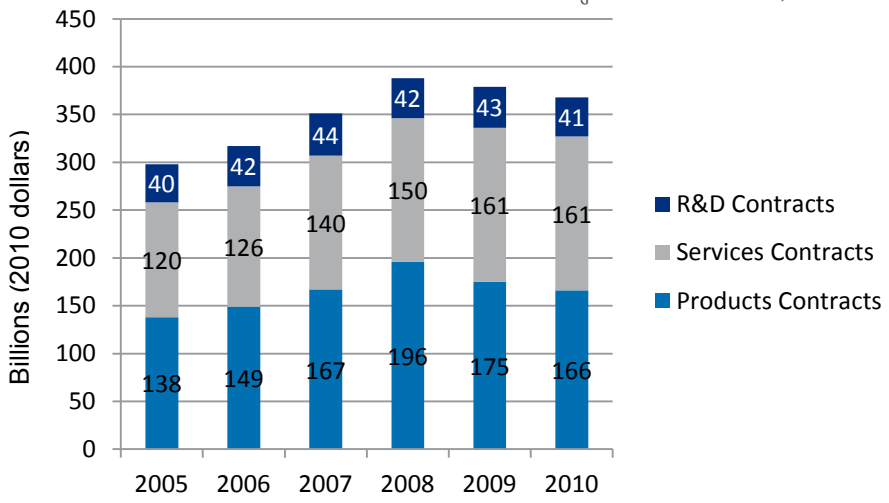
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Defense Industrial Base Sector
Sector Risk Snapshot

The Defense enterprise is the largest and most complex organization in the world. In addition to managing roughly three million employees, a budget of more than $600 billion, operating almost 5,000 locations, and providing healthcare for 9.6 million military members, retirees, and their families, the DOD also executes a multibillion dollar global supply chain that manages an inventory of five million line items.

Figure 1: U.S. Department of Defense Contract Spending and the Supporting Industrial Base

Source: Center for Strategic International Studies, 2011



Defense Industrial Base Sector Goals

Sector Risk Management: Use an all-hazards approach to manage the risk-related dependency on critical DIB assets.

Collaboration, Information Sharing, and Training: Improve collaboration within a shared knowledge environment in the context of statutory, regulatory, proprietary, and other pertinent information-sharing constraints and guidance.

Personnel Security: Mitigate the risk created by personnel with unescorted physical or logical access to critical DIB assets in conformance with pertinent industry best practices, including regulatory and statutory requirements.

Physical Security: Manage the risk created by threats to and vulnerabilities of critical DIB physical assets.

Information Security [Cybersecurity/Information Assurances (CS/IA)]: Manage risk to information that identifies or describes characteristics or capabilities of DIB critical infrastructure and key resources, or that by nature would represent a high risk/high impact to critical infrastructure, resources, or DIB assets.

Defense Industrial Base Sector Overview

- **The Defense Industrial Base (DIB) is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.**
- **Only a small fraction of DIB facilities are DOD-owned. The government component of DIB consists of certain laboratories, special-purpose manufacturing facilities, capabilities for production of uniquely military material such as arsenals and ammunition plants, and other services.**
- **The private sector component of the DIB consists of hundreds of thousands of independent, competing domestic and foreign companies and supply chains, delivering a vast array of products and services to DOD. DIB defense-related products and services equip, inform, mobilize, deploy, and sustain U.S. military and allied military forces worldwide. The DIB companies also deliver national security products and services to other Federal agencies.**
- **DIB does not include commercial infrastructure, such as communications, transportation, power, or other utilities, which serve as critical dependencies of the DIB Sector.**
- **The DIB Sector vision is to collaboratively eliminate or mitigate unacceptable levels of risk to physical, human, and cyber infrastructures, thus ensuring that DOD continues to fulfill its mission, and that DIB activities supporting national security objectives, public health and safety, and public confidence are effective.**

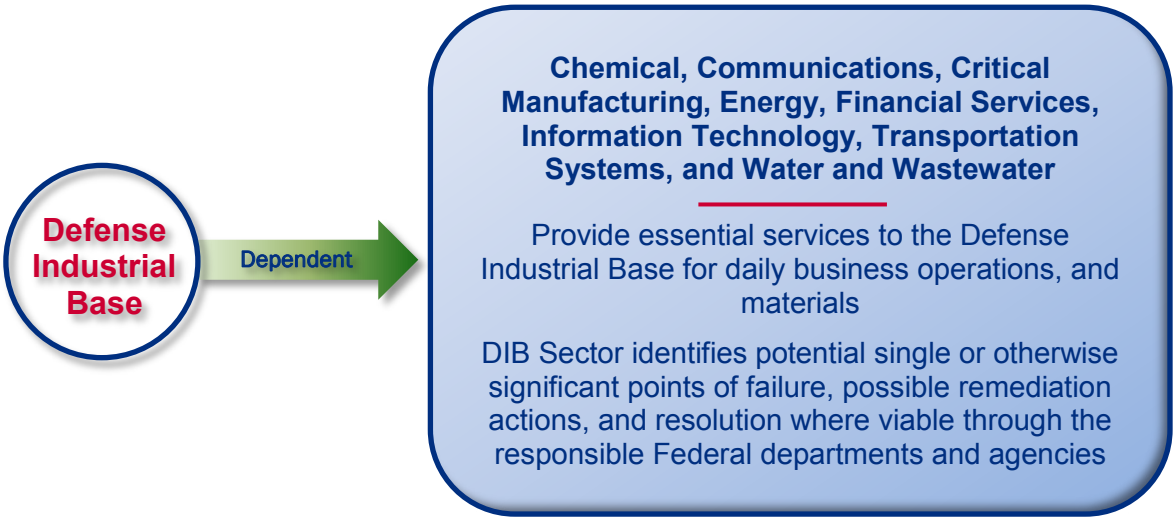
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - The DIB Sector has become heavily dependent on cyber infrastructure, operating within an increasingly information-driven environment.
  - Cyber infrastructure is vulnerable to denial-of-service attacks and malicious modification of information, along with more mundane yet disruptive events, such as system malfunctions, power outages, and human error.
  - These vulnerabilities, combined with the increasing frequency and severity of cyberattacks across the critical infrastructure community, contribute greatly to the risk to the Sector. Foreign entities and non-state actors are also expected to continue seeking to acquire access to sensitive and classified DIB Sector information and technologies by expanding their cyber-collection activities [DOD, *Strategy for Operating in Cyberspace*, July 2011].
- **Loss of Supply Chain Integrity**
  - Due in part to a lack of traceability from foreign producers, potential loss of supply chain integrity (including related manufacturing and material availability) increases risk for the Sector.
  - This is highlighted by the ongoing infiltration of counterfeit electronics into the Sector. Lack of supply chain integrity could lead to the introduction of counterfeit materials, components, and technology into military equipment, which could, in turn, lead to equipment failures and increase risk in the field.

For More Information

- Sector-Specific Agency: Department of Defense, www.defense.gov
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/defense-industrial-base-sector
- Defense Industrial Base, *Sector Specific Plan (SSP)*, 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf
- DOD, Defense Critical Infrastructure Program (DCIP), http://dcip.dtic.mil/index.html

Figure 2: Common, First-order Dependencies of the Defense Industrial Base Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Energy Sector
Electricity Subsector
Sector Risk Snapshot

Figure 1: U.S. Electric Transmission Grid

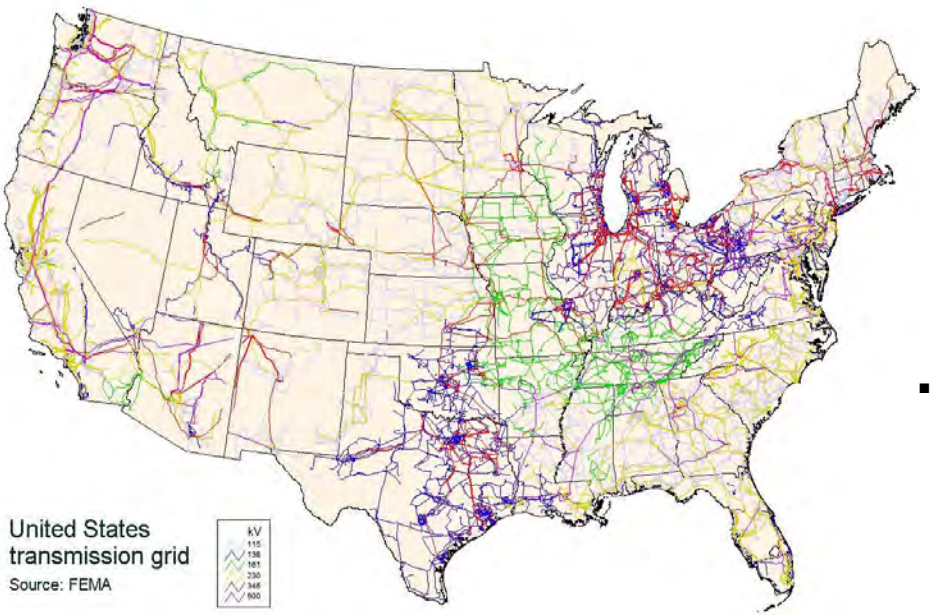
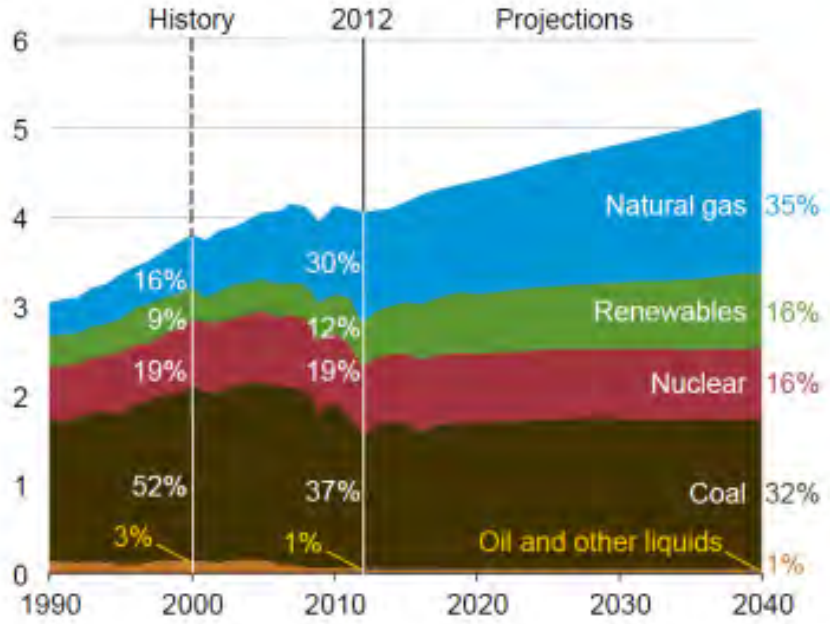


Figure 2: U.S. Electricity Generation by Fuel, 1990-2040 (trillion kilowatt hours)



Source: EIA, *Annual Energy Outlook Early Release Overview*, December 16, 2013, www.eia.gov/forecasts/aeo/er/index.cfm.

Electricity Subsector Overview

- U.S. energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to the Nation's growth and production.
- The Energy Sector is divided into three interrelated segments: electricity, petroleum, and natural gas. According to the Energy Information Administration (EIA), in 2011 there were 18,530 power generation facilities with a combined nameplate capacity of 1,153 gigawatts.
- More than 98 percent of electricity is generated domestically, although some significant regional differences exist and some of the fuels used to generate electricity are imported.
- The primary fuel for electric power generation is coal (37 percent), followed by natural gas (30 percent), nuclear (19 percent), renewable energy sources such as hydro, solar, or wind (12 percent), and other (1 percent). (Source: EIA, 2013)
- The electricity infrastructure is highly automated and controlled by utilities and regional grid operators, using sophisticated energy management systems, such as supervisory control and data acquisition systems (SCADA) or distributed control systems, to keep the system in balance.
- The reliance of virtually all industries and modes on electric power means that all Sectors have some dependence on the Energy Sector.

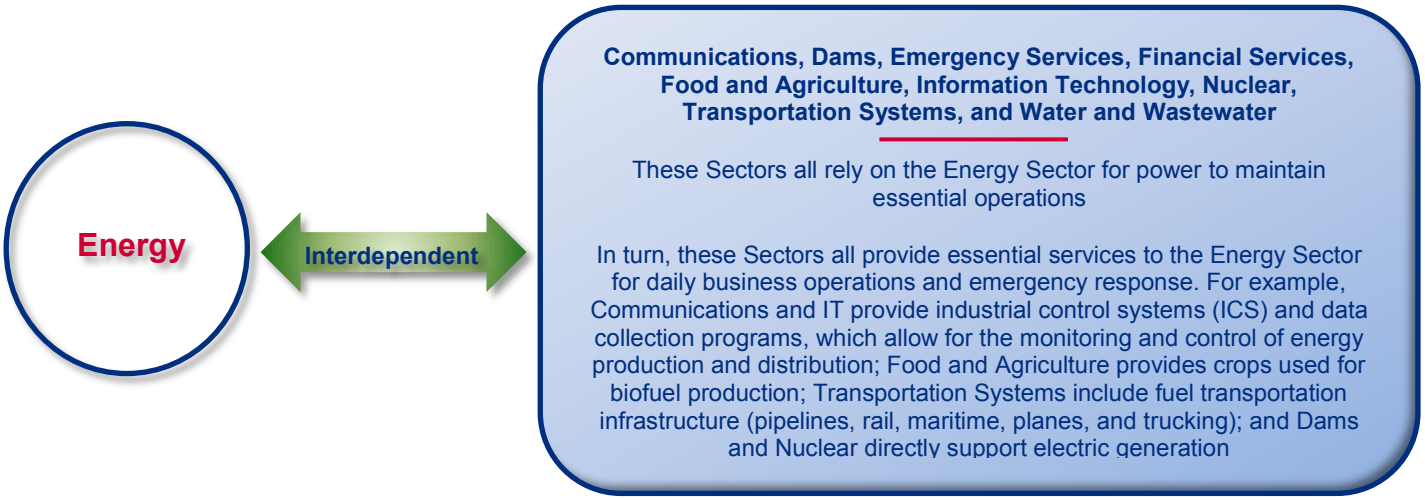
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - Electricity infrastructure is highly automated and controlled by utilities and regional grid operators that rely on sophisticated energy management systems. For example, assets may be vulnerable if the Electricity Subsector's control system networks are connected to the corporate business network, which, in turn, is connected to the Internet. These connections increase the network's vulnerability to direct cyberattacks that could potentially disrupt power and increase risk to the Sector.
  - Insider threats, such as cyber-hacks initiated by current or former employees, increase the risk to the Electricity Subsector. These vulnerabilities are addressed to varying degrees across the Electricity Subsector, through a mix of voluntary and mandatory security standards that apply to electricity grid owners and operators.
- **Physical Attacks**
  - Physical attacks are a risk for the Sector's continued reliable operations. Coordinated physical attacks in the United States could produce wide-ranging impacts to both infrastructure and the reliability of the system.
  - Worldwide, terrorists have executed 2,523 attacks against energy infrastructure since 2004, leaving 1,852 dead and 4,653 wounded (National Counterterrorism Center, *Worldwide Incident Tracking System*, 2011). Moreover, successful strikes against individual Sector assets could lead to regional or nationwide impacts.
- **Natural Disasters**
  - Natural events, such as hurricanes, earthquakes, winter storms, wildfires, and solar flares, are a key risk of the Electricity Subsector, as these events occur regularly and have the capacity to cause extensive and widespread damage, impacting an area from days to weeks.
  - As all other Sectors have some degree of dependency upon the Electricity Subsector for normal operations, electric power restoration is a top priority following a natural disaster.

For More Information

- Sector-Specific Agency: Department of Energy, http://energy.gov/
- EIA, www.eia.gov
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/energy-sector

Figure 3: Common, First-order Interdependencies of the Energy Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

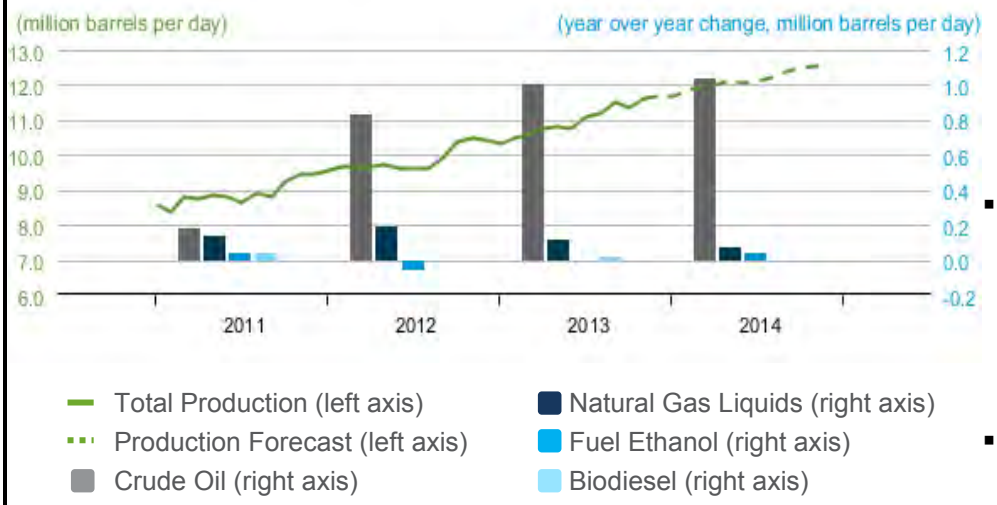
Homeland Security

Energy Sector

Oil and Natural Gas Subsector

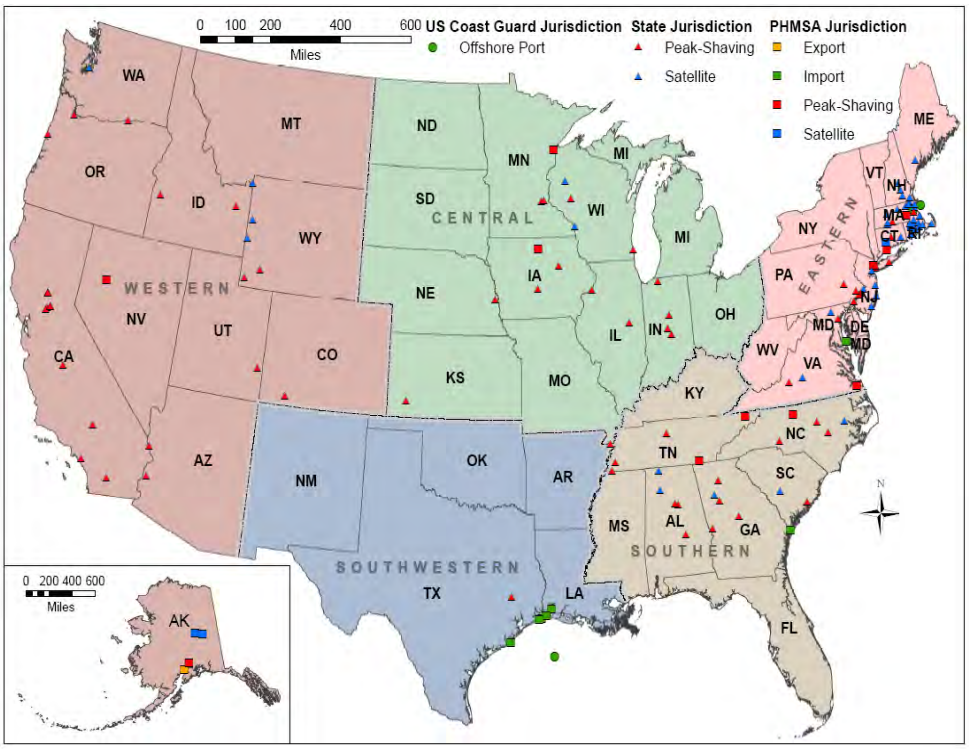
Sector Risk Snapshot

Figure 1: U.S. Crude Oil and Liquid Fuels Production



Source: U.S. Energy Information Administration, Short-Term Energy Outlook, 2013

Figure 2: U.S. Liquefied Natural Gas (LNG) Facilities Connected to Natural Gas Pipeline Systems



Source: U.S. Department of Transportation

Oil and Natural Gas Subsector Overview

- The petroleum section entails the exploration, production, storage, transport, and refinement of crude oil. The crude oil is refined into petroleum products that are then stored and distributed to key economic sectors throughout the United States.
- Key petroleum products include motor gasoline, jet fuel, distillate fuel oil, residual fuel oil, and liquefied petroleum gases. In the United States, there are more than 536,000 crude oil-producing wells, 30,000 miles of gathering pipeline, and 55,000 miles of crude oil pipeline.
- There are 150 operable petroleum refineries, 64,000 miles of product pipeline, and over 1,400 petroleum terminals.
- Natural gas is produced, piped, stored, and distributed in the United States. Imports of liquefied natural gas (LNG) fell 23 percent in 2012 due to unprecedented levels of domestic natural gas production, and companies are now applying to the Department of Energy to export domestic LNG to foreign countries. There are more than 514,000 gas production and condensate wells and 19,000 miles of gathering pipeline in the United States. There are almost 304,000 miles of interstate and intrastate pipeline for the transmission of natural gas.
- Natural gas is distributed to homes and businesses over 1,200,000 miles of distribution pipelines. The heavy reliance on pipelines to distribute products across the Nation highlights the interdependencies between the Energy and Transportation Systems Sectors.
- The reliance of virtually all industries and modes on fuels means that all Sectors have some dependence on the Energy Sector.

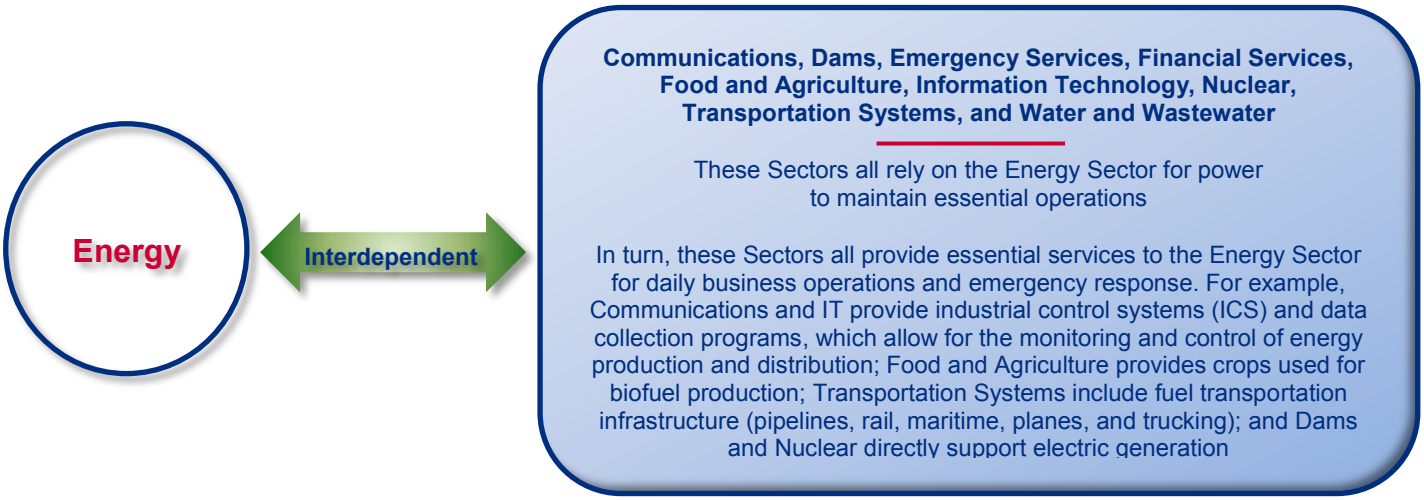
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - Oil and natural gas infrastructure is highly automated and controlled by pipeline operators, terminal owners, and natural gas utilities that rely on sophisticated energy management systems. Assets may be vulnerable if these industrial control systems are connected to the Internet, either directly or indirectly. For example, control system networks may be connected to the corporate business network, which, in turn, is connected to the Internet. These connections increase the network's vulnerability to direct cyberattacks that could potentially disrupt movement and increase risk to the Sector.
  - Insider cyberthreats, such as those initiated by current or former employees, create risk to the Oil and Natural Gas Subsector. Cyber-actors can target industrial control systems (ICS) and gain control of a process within a refinery, pipeline, or terminal. A cyber-actor could manipulate the production, storage, and transportation aspects of oil and natural gas. These vulnerabilities are addressed to varying degrees across the Oil and Natural Gas Subsector, through a mix of voluntary and mandatory security standards that apply to owners and operators.
- **Physical Attacks**
  - Physical attacks are a risk for the Sector's continued reliable operation. Coordinated physical attacks in the United States could produce wide-ranging impacts to both infrastructure and the reliability of the system.
  - Worldwide, terrorists have executed 2,523 attacks against energy infrastructure since 2004, leaving 1,852 dead and 4,653 wounded (National Counterterrorism Center, *Worldwide Incident Tracking System*, 2011). Successful strikes against individual Sector assets could lead to cascading regional or nationwide impacts.
- **Natural Disasters**
  - Many natural disasters can affect the Oil and Natural Gas Subsector. Hurricanes are the most frequent disruptive natural hazard for the Subsector, often causing the preemptive shutdown of facilities in an area, even if the facilities themselves are not directly affected by the storm. Hurricanes Ike and Gustav impacted almost 65 million barrels of crude oil production and 400 billion cubic feet of the natural gas supply (Energy Information Administration, *2010 Outlook for Hurricane-Related Production Outages in the Gulf of Mexico*, 2010).

For More Information

- Sector-Specific Agency: Department of Energy, http://energy.gov/
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/energy-sector
- U.S. Department of Pipeline and Hazardous Materials Safety Administration (PHMSA), www.phmsa.dot.gov

Figure 3: Common, First-order Interdependencies of the Energy Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Emergency Services Sector Sector Risk Snapshot

Function/Discipline	Roles and Responsibilities
Law Enforcement	Maintaining law and order and protecting the public from harm. Law enforcement activities may include investigation, prevention, response, court security, and detention, as well as other associated capabilities and duties.
Fire and Emergency Services	Prevention and minimizing loss of life and property during incidents resulting from fire, medical emergencies, and other all-hazards events.
Emergency Medical Services	Providing emergency medical assessment and treatment at the scene of an incident, during an infectious disease outbreak, or during transport and delivery of injured or ill-individuals to a treatment facility as part of an organized EMS system.
Emergency Management	Leading efforts to mitigate, prepare for, respond to, and recover from all types of multijurisdictional incidents.
Public Works	Providing essential emergency functions, such as assessing damage to buildings, roads, and bridges; clearing, removing, and disposing of debris; restoring utility services; and managing emergency traffic.

Emergency Services Infrastructure

- Large, geographically distributed base of facilities, equipment, and highly skilled personnel who provide services in both paid and volunteer capacities.
- Largely organized at the State, local, tribal, and territorial levels of government, corresponding to the scales on which emergencies generally occur. The complex and dispersed nature of the Sector makes it difficult to disable the entire system; it also presents challenges in coordinating emergency responses across disciplines, regions, and levels of government.
- Relies heavily on complex communication and information technology systems to enable robust communications and appropriate coordination and management of diverse elements during emergency situations.
- Uses specialized transportation vehicles and secure transportation routes to facilitate Sector operations because personnel, equipment, aid, and victims must be moved to and from scenes of emergencies.
- The Sector focuses primarily on the protection of other sectors and people, rather than protecting the Sector itself, which presents unique challenges in addressing the protection of Emergency Services as a critical infrastructure sector.
- ESS involves primarily the public sector, but also includes private sector holdings, such as industrial fire departments, sworn private security officers, and private EMS providers.

Emergency Services Sector Overview

- **The Emergency Services Sector (ESS) comprises five disciplines: Law Enforcement, Fire and Rescue Services, Emergency Medical Services (EMS), Emergency Management, and Public Works.**
- **In addition, there are specialized capabilities: Explosive Ordnance Disposal, Hazardous Materials Response, Special Weapons and Tactics and Tactical Operations, Search and Rescue, Aviation Units, and Public Safety Answering Points.**
- **Through partnerships with public and private sector entities, this Sector's mission is to save lives, protect property and the environment, assist communities impacted by disasters (natural or manmade), and aid recovery from emergency situations.**
- **ESS assets, systems, networks, and functions are critical to maintain, protect, and preserve the Nation's safety and health in case of naturally occurring or manmade threats and hazards. By protecting these elements, the Sector is better able to support all critical infrastructure, essential governmental missions, and public services.**
- **The Sector has dependencies and interdependencies with multiple critical infrastructure sectors and the National Response Framework's Emergency Support Functions that support both ESS operations and protection of ESS assets.**

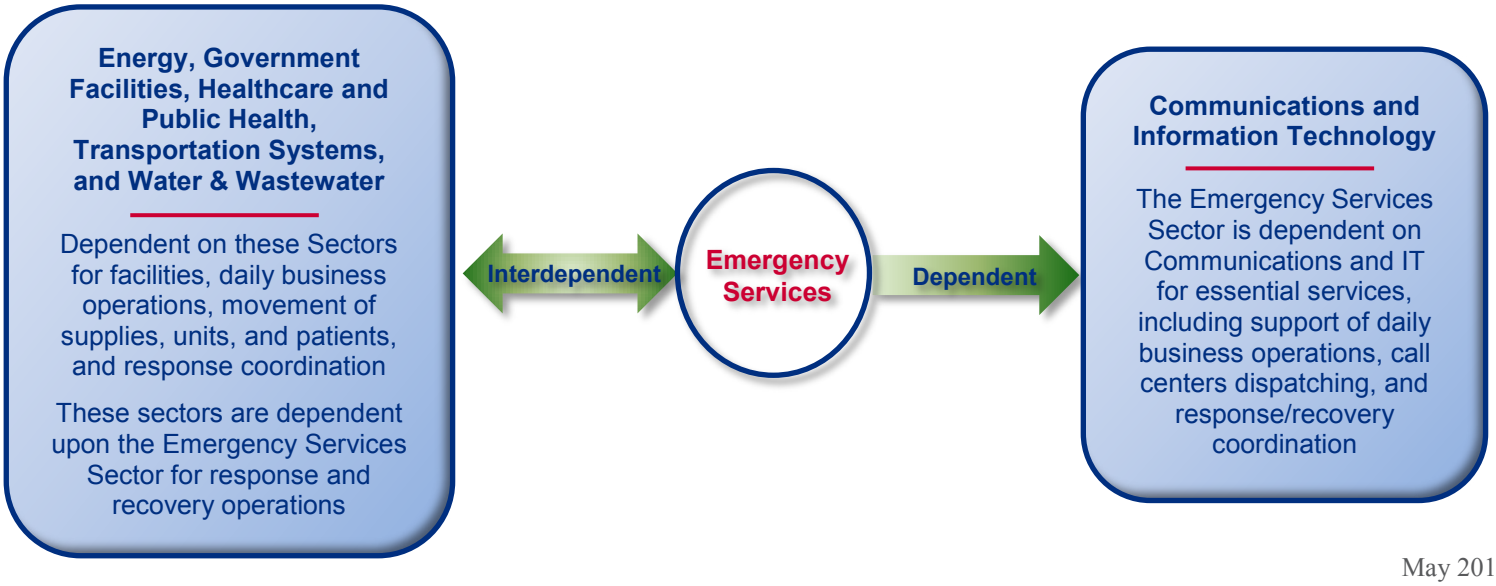
Threats and Hazards of Significant Concern

- **Communications Vulnerabilities**
  - Communication channels and equipment standards have improved dramatically in the last several years. However, many jurisdictions still struggle to use standardized emergency call codes and police radio codes, have difficulty obtaining bandwidth to transmit communications, lack interoperable communications equipment, and do not share frequencies among the various member organizations of the Sector (e.g., police and fire). All of these contribute to ongoing risk for the Sector.
- **Cyberthreats**
  - The dependence of the ESS on information technology also contributes to risk. For example, cyberdisruption of communications systems, computer networks in service vehicles, or GPS during an emergency operation could dramatically disrupt or delay the initial response to an event.
- **Malicious Actors**
  - Contribute significant risk to the Sector. Fire, police, hazardous materials, and other emergency service units respond to criminal threats, violent extremists, suspected terrorist events (e.g., mailed letters and packages containing white powders that could be anthrax), and the aftermath of terrorist attacks (e.g., the bombing of the Oklahoma City Murrah Federal Building, the events of September 11, 2001, and the anthrax events of 2001).
  - As a result, emergency services personnel are exposed to substances of unknown composition, for which their personal protective equipment may not provide adequate protection and from which there may be long-term health implications. Adversaries may also target persons in positions of authority, as well as institutions that are symbolic of a functioning society. ESS representatives may be attacked with improvised explosive devices or targeted by active shooters for these same reasons.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/about-office-infrastructure-protection
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/emergency-services-sector

Figure 1: Common, First-order Dependencies and Interdependencies of the Emergency Services Sector



May 2014

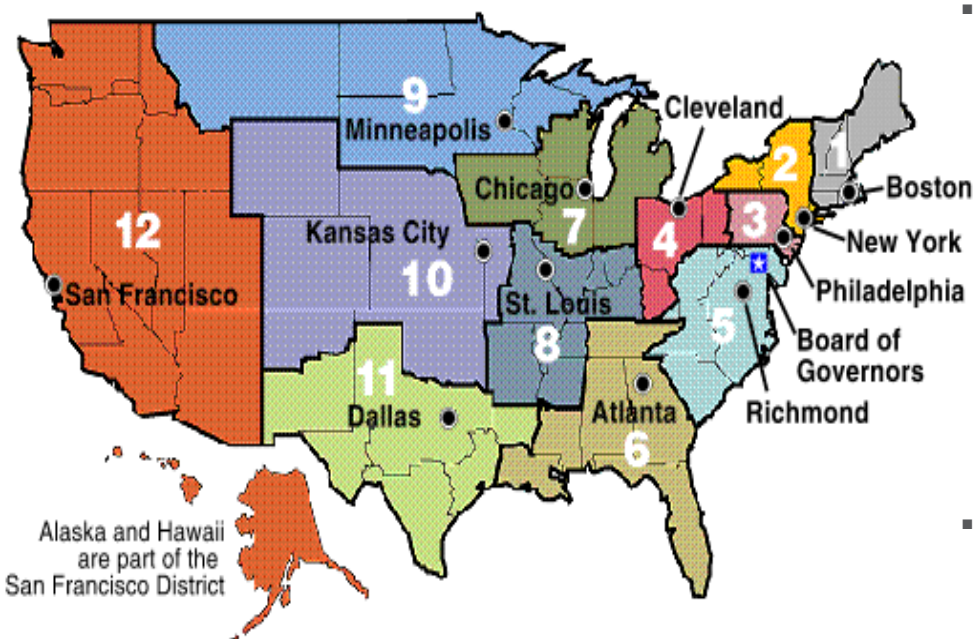
Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

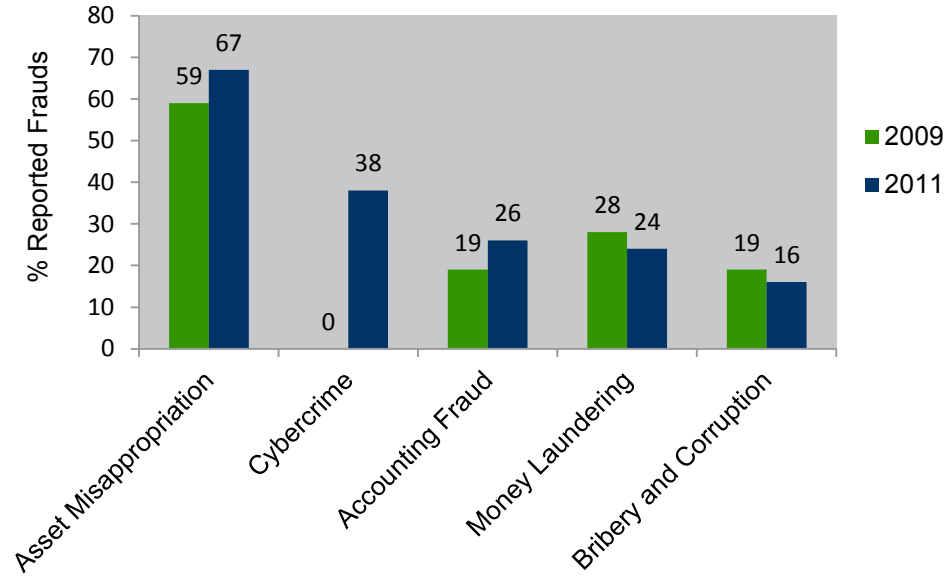
Financial Services Sector
Sector Risk Snapshot

Figure 1: U.S. Federal Reserve Bank Locations and Districts



Source: The Federal Reserve Board, www.federalreserve.gov/otherfrb.htm

Figure 2: Top 5 Types of Economic Crimes Experienced by the Financial Services Sector, as Reported in a PwC 2011 Global Survey



Source: PricewaterhouseCoopers, LLP, *Fighting Economic Crime in the Financial Services Sector,* 2012, www.pwc.com/en_GX/gx/economic-crime-survey/pdf/fighting-economic-crime-in-the-financial-services-sector.pdf

Financial Services Sector Overview

- The Financial Services Sector represents a vital component of the Nation's critical infrastructure. As the Sector-Specific Agency, the Department of the Treasury works with all relevant Federal Departments and agencies; State, local, and tribal governments; and the private sector to promote efforts to improve the Sector's ability to prepare for, respond to, prevent, and mitigate manmade threats, natural disasters, and other intentional or unintentional risks.
- Financial institutions provide a broad array of products from the largest institutions to the smallest community banks and credit unions. These products allow customers to do the following:
  - Deposit funds and make payments to other parties;
  - Provide credit and liquidity to customers;
  - Invest funds for both long and short periods; and
  - Transfer financial risks between customers.
- Financial institutions are organized and regulated, based on services provided by institutions. Within the sector, there are more than 18,800 federally insured depository institutions; thousands of providers of various investment products, including roughly 18,440 broker-dealer, investment adviser, and investment company complexes; providers of risk transfer products, including 7,948 domestic U.S. insurers; and thousands of other credit and financing organizations.

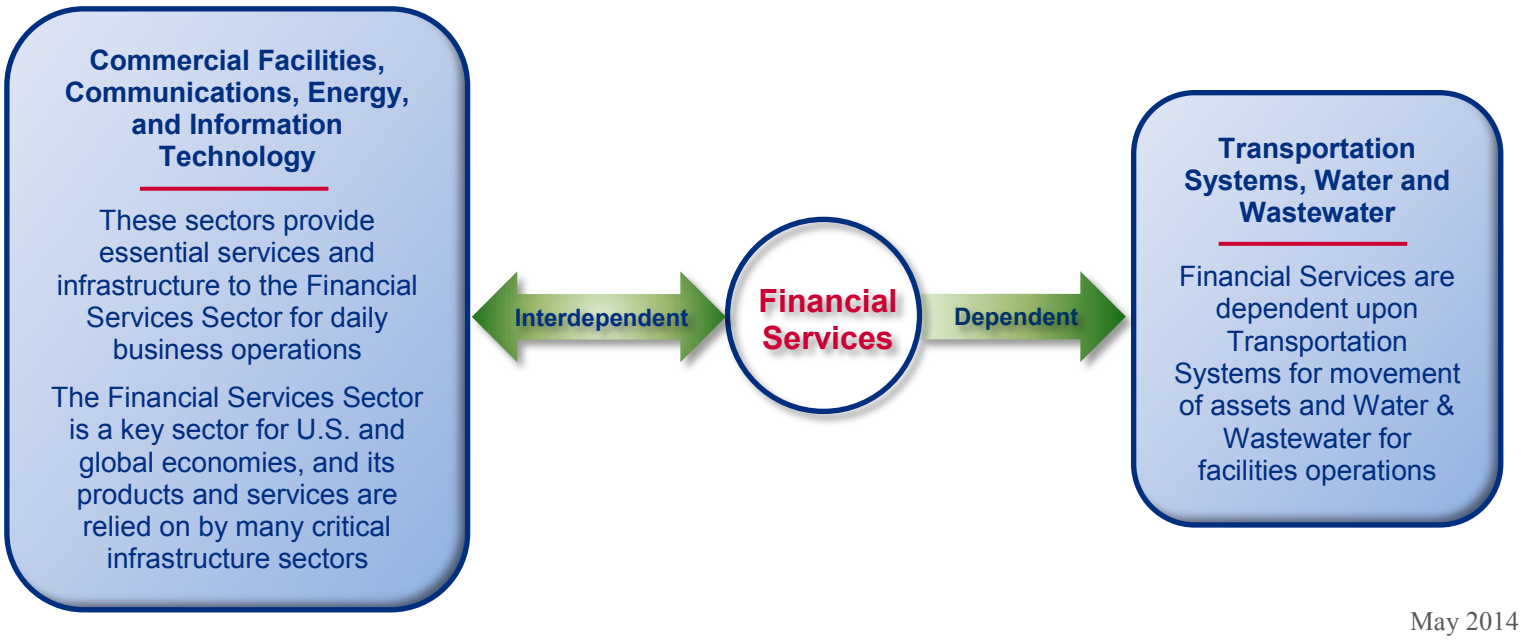
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - Terrorists, transnational criminals, and foreign intelligence services are becoming aware of and using computer viruses, Trojan horses, worms, logic bombs, eavesdropping sniffers, and other tools that can destroy, intercept, degrade the integrity of, or deny access to data.
  - Other potential cyberthreats to the Sector include confidentiality and identity breaches, emerging technology, professionalization of cyber-criminals, and continued globalization of the Sector.
- **Insider Threats**
  - These threats could come from individuals or groups with malicious intent, including but not limited to disgruntled employees and organized crime members, or those with unwitting intent.
  - Insider threats pose a significant concern since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage, steal, and/or move assets without possessing a great deal of knowledge about computer intrusions. Unwitting employees or third parties may also unintentionally damage, destroy, or steal data.
- **Large-scale Physical Events**
  - Natural hazards or terrorist attacks could cause significant economic losses to the Sector and to the Nation.
  - Regulators responsible for safety and soundness of financial services issue guidelines and specific regulations requiring redundancy and security in physical and financial systems. They have long required banking institutions to address operating and security risks in their contingency plans.

For More Information

- Sector-Specific Agency: Department of the Treasury, www.treasury.gov
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, www.dhs.gov/banking-and-finance-sector
- Financial Services Information Sharing and Analysis Center (FS-ISAC), https://www.fsisac.com/

Figure 3: Common, First-order Dependencies and Interdependencies of the Financial Services Sector



May 2014

Homeland Security
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Food and Agriculture Sector Sector Risk Snapshot

FOOD DEFENSE

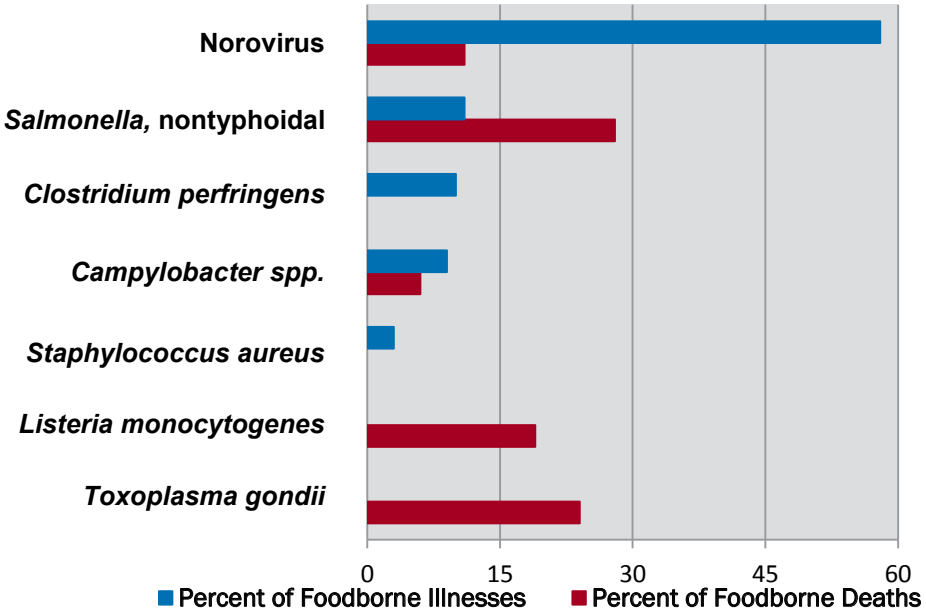
Activities associated with protecting the Nation's food supply from deliberate or intentional acts of contamination or tampering. This term encompasses other similar verbiage (e.g., bioterrorism or chemicalterrorism).

FOOD SAFETY

Activities associated with preventing the accidental contamination of food products by biological, chemical, or physical hazards. Focuses on the proper handling and preparation of food and agricultural products.

Figure 1: Top Pathogens Contributing to Domestically Acquired Foodborne Illnesses and Deaths, 2000-2008.

The Centers for Disease Control and Prevention (CDC) estimates that each year 1 in 6 Americans (or 48 million people) get sick, 128,000 are hospitalized, and 3,000 die of foodborne diseases.



Source: CDC, *2011 Estimates of Foodborne Illness in the United States*, www.cdc.gov/foodborneburden/2011-foodborne-estimates.html

FOOD AND AGRICULTURE SECTOR OVERVIEW

- **The Food and Drug Administration (FDA) and U.S. Department of Agriculture (USDA) jointly serve as the Sector Specific Agencies for the Food and Agriculture Sector.**
- **Composed of complex production, processing, and delivery systems and encompasses upwards of 4 million assets, including 2 million+ farms, 900,000+ restaurants, 100,000+ food retail establishments. As of February 19, 2014, there were 81,575 FDA registered domestic food facilities (warehouses, manufacturers, processors) and 115,753 FDA registered foreign food facilities. USDA regulates 6,805 establishments, including establishments for meat, poultry, processed egg products, imported products, and voluntary inspection services.**
- **Accounts for roughly one-fifth of the Nation's economic activity.**
- **The open nature and global interconnectivity of the sector presents unique security challenges, and leaves the sector vulnerable to a variety of all-hazards threats, including severe weather, pests and disease, and contamination with biological, chemical, or radiological agents.**
- **Direct attacks on the sector, such as the introduction of animal or plant disease, or deliberate food contamination, could result in devastating animal, plant, or public health and economic consequences.**

FOOD AND AGRICULTURE INFRASTRUCTURE

- Food and Agriculture Sector infrastructure is unique, complex, broad-based, globally distributed, and highly integrated, and is seen as a system of systems (i.e., systems of individual assets that are closely dependent on each other).
- Many of the sector's systems defy traditional security practices because they are not brick-and-mortar entities, like buildings, bridges, or dams. Instead, they are open areas (i.e., farms, ranches, or livestock transport areas) and complex systems that span the globe.
- Many of these systems face natural threats, including livestock and crop diseases and foodborne pathogens, thus monitoring, early threat detection, and rapid response are key mitigation activities for the sector.
- Food and agriculture owners and operators must anticipate the possibility of a terrorist attack on their products and evaluate their preparedness and mitigation strategies to either thwart an attack or, at the very least, mitigate the damage, and recover from the animal, plant, public health, economic, and psychological impacts of an attack.

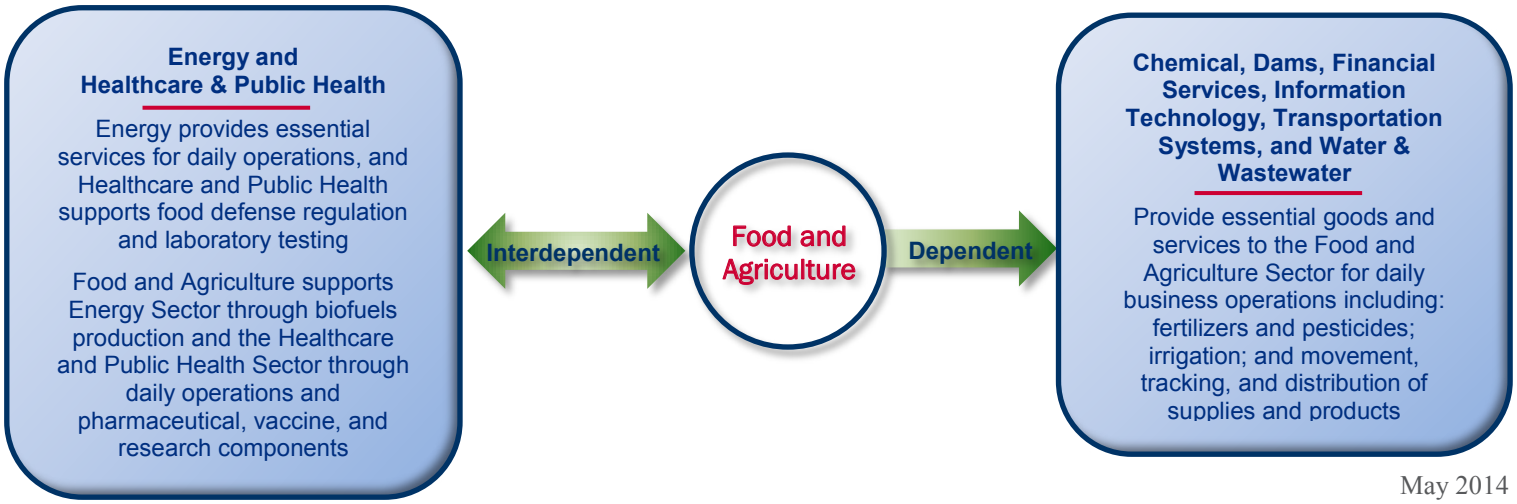
Threats and Hazards of Significant Concern

- **Food Contamination (whether by accidental or intentional means)**
  - Contaminated food in the United States is estimated to be responsible for over 47.8 million illnesses, 127,839 hospitalizations, and 3,037 deaths, costing the Nation more than $14 billion a year in terms of medical care, lost productivity, chronic health problems, and deaths (CDC, 2011).
  - Violent extremists and terrorists have indicated an interest in poisoning the food supply with biological and chemical agents, which has great potential to cause costly economic losses in the supply chain for implicated foodstuffs, creating public panic, and leading to a public health crisis with considerable mortality and morbidity (FBI, www.fbi.gov/stats-services/publications/law-enforcement-bulletin/february-2012/agroterrorism, 2012).
- **Disease and Pests**
  - The accessibility of crops and animals on the farm and the extensive international and interstate movement of animals and products increase the sector's vulnerability to rapidly spread disease.
  - Modeling estimates and historical evidence demonstrate that a domestic outbreak of a foreign animal disease, such as Foot and Mouth Disease, could cost the United States billions of dollars due to loss of livestock, production, and international trade.
- **Severe Weather (including droughts, floods, and climate variability)**
  - Natural hazards are an important risk to the Food & Agriculture Sector, and critically influence farm productivity.
  - Weather and climate characteristics such as temperature, precipitation, and water availability directly impact the health and well-being of plants and livestock, as well as pasture and rangeland production.
  - The harmful effects of severe weather coupled with global climate change are currently affecting U.S. water resources, agriculture, land resources, and biodiversity. This trend is expected to continue (USDA, 2013, www.usda.gov/oce/climate_change/effects.htm).

For More Information

- Sector-Specific Agencies: U.S. Department of Agriculture (USDA), Office of Homeland Security and Emergency Coordination, National Security Policy Staff, www.dm.usda.gov/ohsec/rpd/index.htm; and Department of Health and Human Services Food and Drug Administration (FDA), *Food Defense and Emergency Response*, www.fda.gov/Food/FoodDefense/default.htm
- DHS,www.dhs.gov/food-and-agriculture-sector
- DHS, *IP Note: Reducing the Vulnerability of the U.S. Food Supply to Intentional Contamination*, 10 August 2010
- DHS, USDA, FDA, *2010 Food and Agriculture Sector Specific Plan*, ww.dhs.gov/files/programs/gc_1179866197607.shtm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies and Interdependencies of the Food & Agriculture Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Government Facilities Sector
Sector Risk Snapshot

Government Facilities Security Levels

Because of the differences among Federal buildings and their security needs, U.S. Federal Marshals Services categorized Federal facilities into five classes based on building size, agency mission and function, tenant population, and the degree of public access to the facility, and developed security standards corresponding to the security level needed for each class.

Level I—buildings with no more than 2,500 square feet, 10 or fewer Federal employees, and limited or no public access

Level II—buildings with 2,500 to 80,000 square feet, 11 to 150 Federal employees, and moderate public access

Level III—buildings with 80,000 to 150,000 square feet or more, 151 to 450 Federal employees, and a moderate-to-high public access

Level IV—buildings with 150,000 square feet or more, more than 450 Federal employees, and a high level of public access

Level V—buildings that are similar to Level IV but are considered critical to national security

Critical Infrastructure Security and Resilience Issues

- Government facilities represent attractive and strategically important targets for both domestic and international terrorist groups, as well as criminals.
- These assets are often targeted because they provide unique services, often perform sensitive functions, and have significant symbolic value.
- Because of the high-profile nature of the sector, government facilities operate within a very dynamic risk environment requiring a variety of well-coordinated protective measures to ensure the safety and security of citizens and the continued availability of essential government functions.

Government Facilities Sector Overview

- **Comprises a wide variety of buildings, national monuments, and icons in the United States and overseas that are owned or leased by Federal, State, local, and tribal governments.**
- **The sheer size and scope of the Government Facilities Sector poses a challenge in providing for infrastructure protection efforts.**
- **The Federal Government alone manages approximately 3.35 billion square feet of space and more than 650 million acres of land across the United States. The Sector also includes the facilities owned and operated by the more than 87,000 municipal governments across the Nation and abroad.**
- **These facilities include general-use office buildings and special-use military installations, embassies, courthouses, and national laboratories that contain highly sensitive information, materials, processes, and equipment.**
- **Many government facilities are open to the public for business activities, commercial transactions, or recreational activities, while others are not.**
- **The Government Facilities Sector includes the Education Facilities Subsector, which covers pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools.**
- **The National Monuments and Icons Subsector was consolidated within the Government Facilities Sector in 2013 under Presidential Policy Directive 21. The Subsector encompasses a diverse array of assets, networks, systems, and functions located throughout the United States. Many are listed in either the National Register of Historic Places of the List of National Historic Landmarks.**

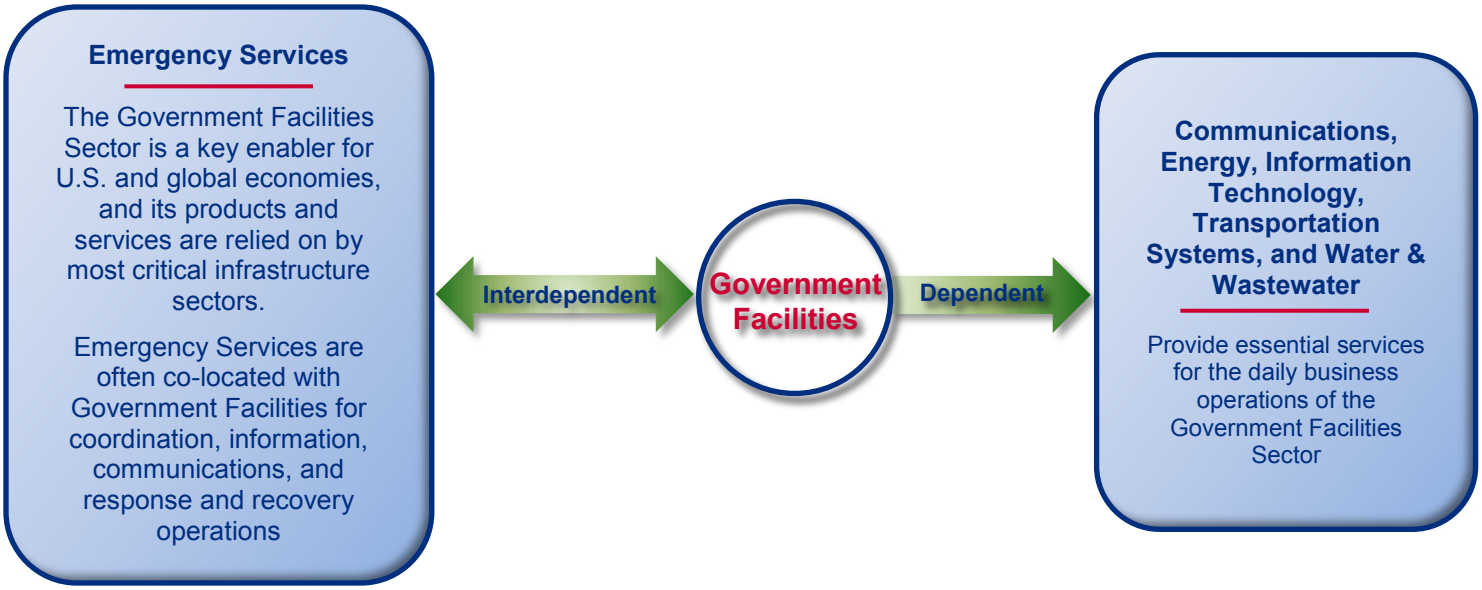
Threats and Hazards of Significant Concern

- **Terrorist Attacks**
  - The threat of terrorist attacks contributes significantly to the risks of the Government Facilities Sector. A major challenge in the protection of government facilities is balancing the need for security with the need for public access to government offices for services and transactions.
  - Global events and trends suggest that terrorists will likely continue to use improvised explosive device tactics—historically one of the most successful tactics—to attack U.S. critical infrastructure. Government facilities may also be targeted by active shooters, as occurred in the 2010 shooting at a Federal courthouse in Las Vegas. (Doherty, R., *Critical Research/Innovation Focus Area Document: Vehicle-Borne Improvised Explosive Devices (VBIED)* Detection, Washington, D.C.: U.S. Department of Homeland Security, Science and Technology Directorate, 2009)
- **Cyberthreats**
  - Cyberintrusions into automated security and supervisory control and data acquisition systems are risks. The increasing reliance on automated security systems and automated building management systems will likely increase vulnerabilities and the likelihood of cyberintrusion, especially in the form of sabotage by current or former insiders with malicious intent.
  - Cyberintrusion into the security systems of government facilities could compromise the protection of facilities, civil servants, and the general public and allow for exploitation and attacks with significant consequences.

For More Information

- Sector-Specific Agency: Department of Homeland Security Federal Protective Service www.dhs.gov/topic/federal-building-security, and the General Services Administration www.gsa.gov
- Government Facilities Sector, www.dhs.gov/government-facilities-sector
- National Infrastructure Protection Plan, www.dhs.gov/nipp
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- Contact NIPP@hq.dhs.gov or NIPP-GFS@hq.dhs.gov

Figure 1: Common, First-order Dependencies and Interdependencies of the Government Facilities Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Government Facilities Sector
Education Facilities Subsector
Sector Risk Snapshot

The Principles of School Emergency Management Planning
Must be supported by leadership. At the district and school levels, senior-level officials can help the planning process by demonstrating strong support for the planning team.
Uses assessments to customize plans to the building level. Effective planning is built around comprehensive, ongoing assessment of the school community, which customizes plans to the building level, taking into consideration the school's unique circumstances and resources.
Considers all threats and hazards. The planning process must take into account a wide range of possible threats and hazards that may impact the school, addressing safety needs before, during, and after an incident.
Provides for the access and functional needs of the whole school community. The "whole school community" includes children, individuals with disabilities and others with access and functional needs, those from religiously, racially, and ethnically diverse backgrounds, and people with limited English proficiency.
Considers all settings and all times. School EOPs must account for incidents that may occur during and outside the school day as well as on and off campus (e.g., sporting events, field trips).
Creating and revising a model Emergency Operations Plan is done by following a collaborative process.
Source: U.S. Department of Education, Readiness and Emergency Managements for Schools Technical Assistance Center, http://rems.ed.gov/Default.aspx (2014).

Number of U.S. Educational Institutions by Number and Control of Institution	
Public Schools (2012)	**98,328**
Elementary	66,689
Secondary	24,357
Combined	6,311
Other[1]	971
Private Schools (2011)	**30,860**
Postsecondary Title IV Institutions (2013)	**7,253**
Degree-granting institutions	4,726
2-year colleges	1,700
4-year colleges	3,026

[1]Includes special education, alternative, and other schools not classified by grade span

Source: U.S. Department of Education, National Center for Education Statistics, *2013 Digest of Education Statistics* (2014, Advance Release).

Education Facilities Subsector Overview

- **The Education Facilities Subsector (EFS) encompasses pre-kindergarten (pre-K) through 12th grade and post-secondary public, private, and proprietary education facilities.**
- **The Department of Education serves at the Sector-Specific Agency for the Education Facilities Subsector.**
- **EFS assets and systems vary dramatically and include rural and urban, public and private education facilities ranging from fewer than a hundred students to many thousands of students. EFS assets also include pre-K through 12 and higher education campus grounds, increasing the number of facilities, the level of complexity, and the challenges to risk mitigation.**
- **The overall EFS vision is that all education facilities are ready to prevent, mitigate, prepare for, respond to, and recover from any natural or manmade hazard, by having a comprehensive, all-hazards plan to enhance safety, minimize disruption, and ensure continuity of the learning environment.**
- **For the EFS, comprehensive, all-hazards emergency management plans are the appropriate approach to mitigating risk and enhancing resilience for all of EFS' human, physical, and cyber assets.**
- **Comprehensive plans are based on the four phases of school emergency management (prevention and mitigation, preparedness, response, and recovery). Such plans are practiced and updated regularly, coordinated with appropriate State and local partners, and developed in close collaboration with first responders and the community.**
- **They include written plans for an infectious disease outbreak, support the National Incident Management System, contain measures to address food defense, and incorporate students and staff with special needs.**

Threats and Hazards of Significant Concern

- **Natural Hazards** (e.g., hurricanes, wildfires)
  - Weather events pose a risk to the safety of the personnel and students at these institutions. Significant damage can cause the institution to close in the short and long term.
- **Public Health Hazards** (e.g., Methicillin-Resistant Staphylococcus Aureus (MRSA), salmonella outbreaks , H1N1, and intentional adulteration of food)
  - Public health hazards pose a risk to the safety of the personnel and students at these institutions. Significant damage can cause the institution to close in the short and long term.
- **Active Shooter** (e.g., Columbine, Virginia Tech, and Sandy Hook Elementary School)
  - Shootings pose a threat to the safety of the personnel and students at these institutions. Schools are targets because shootings bring national attention to the individual or group. Public confidence and the continuity of school operations could be negatively affected.
- **Cyberthreats** (e.g., computer system hacking, phishing)
  - Higher education institutions often collect and store sensitive, personal student data and databases (Social Security numbers, health, financial, and educational data). Education facilities with emergency management data housed electronically require cybersecurity efforts to maintain the integrity of their plans (i.e., emergency management plans, floor plans).
  - Disruptions to institutional data systems could impact the capacity to effectively perform essential business operations and could cause a temporary to long-term school closure.
  - Although a cyberattack on an education facility would not likely impose cascading effects for the Nation, it can have such effects on the campus community through the compromise of personal data, security systems, and research facilities that rely on cyber elements or of emergency management data housed electronically.

For More Information

- Sector-Specific Agency: The Department of Education, www.ed.gov
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS, 2010 Education Facilities Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-education-facilities-2010.pdf
- Readiness and Emergency Management for Schools, http://rems.ed.gov/

Figure 1: Common, First-order Dependencies of the Education Facilities Subsector

May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Healthcare and Public Health Sector

Sector Risk Snapshot

Healthcare and Public Health Sector Overview

- **The Healthcare and Public Health (HPH) Sector is the lead Sector responsible for protecting and sustaining the Nation's health. The U.S. Department of Health and Human Services (HHS) serves as the Sector-Specific Agency for the HPH Sector.**
- **This widespread and diverse Sector includes acute care hospitals, ambulatory healthcare, public-private financial systems, Federal, State, and local public health systems; disease surveillance; and private sector industries that manufacture, distribute, and sell drugs, biologics, and medical devices.**
- **The Sector is vulnerable to a variety of all-hazards threats, and is especially concerned about potentially catastrophic impacts resulting from biological, cyber, vehicle-borne explosive devices, and insider threats.**
- **Such attacks could result in large numbers of illness and casualties, denial of service, or theft of confidential patient information.**
- **For the Sector, critical infrastructure protection is ultimately defined by the extent to which the Sector has been able to mitigate interruptions in the delivery of healthcare and public health services.**

Figure 1: Occurrence of Major Flu Pandemic or New Influenza Strain over the Past 100 years

Major pandemic Appearance of a new influenza strain in the human population

Table 1: Major Flu Pandemics in the Past 100 Years, with Comparison to Seasonal Flu

	Virus Strain	First Identified	Ground Zero	Higher Risk/Age Group	Estimated Infection Rate	Mortality Rate	Estimated Deaths
Seasonal Flu	Seasonal variation	Seasonal variation	N/A	Very young, very old, and the infirm	5-15%	0.6%	0.25-0.5 million
Spanish Flu	H1N1	Spring 1918	Western Europe	Age 20-50	20-40%	2-2.5%	40-50 million
Asian Flu	H2N2	February 1957	China	School-aged children, elderly	30%	0.025%	2-4 million
Hong Kong Flu	H3N2	Early 1968	Hong Kong	Elderly	30%	0.02%	1-3 Million
Influenza A (H1N1)	H1N1	April 2009	Mexico	Children, teens, young adults	24%[1]	0.02%[1]	>18,500[1]

[1] World Health Organization (WHO), "Estimating age-specific cumulative incidence for the 2009 influenza pandemic: a meta-analysis of A(H1N1)pdm09 serological studies from 19 countries," *Influenza and Other Respiratory Viruses*, Vol:7, January 2013

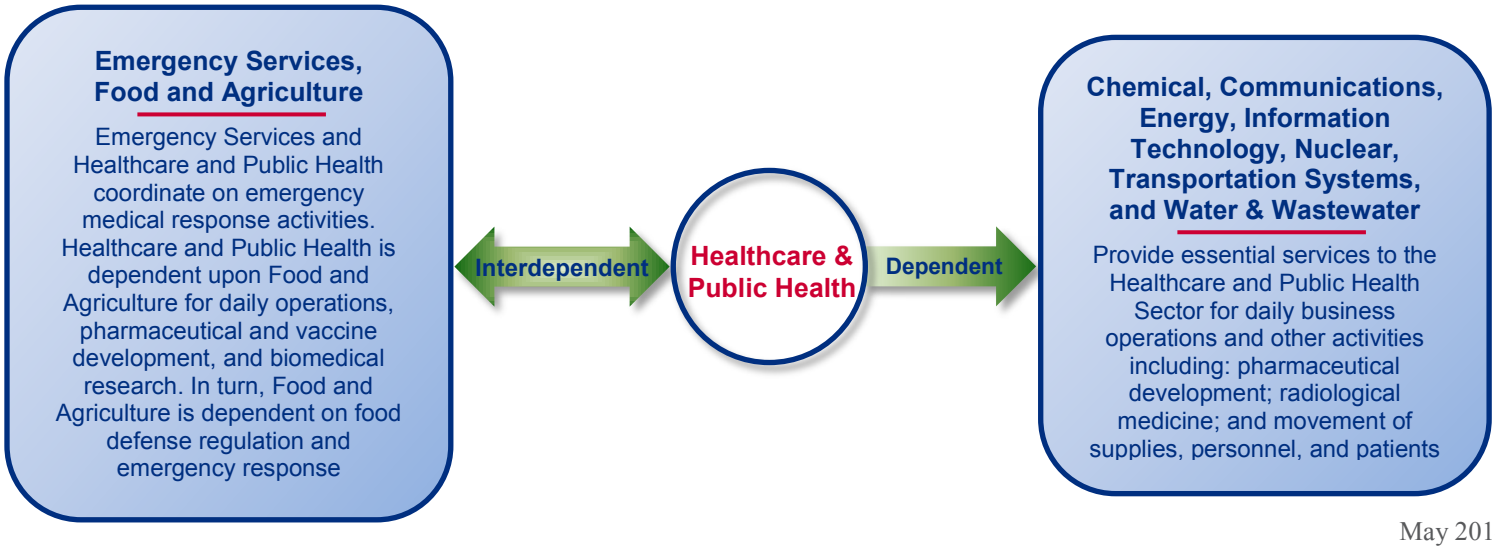
Threats and Hazards of Significant Concern

- **Global Supply Chain Disruptions**
  - A supply chain disruption refers to an event leading to a shortage of a pharmaceutical, device, or biologic. A natural disaster may make roads impassable and thereby prevent goods from arriving at an effected area, or a product may be contaminated at its place of origin and need to be recalled resulting in a limited amount of that product on the market.
  - Independent of the reason, supply chain disruptions can be catastrophic, as healthcare providers tend to rely on just-in-time resupplying and therefore do not always have sufficient stockpiles to weather a delay, especially during events that lead to an increased demand for healthcare or healthcare-related products.
- **Theft and Exploitation of Medical Goods and Confidential Medical Information**
  - Theft and exploitation result from the work of malicious actors.
  - Many medical facilities and laboratories contain radiological materials or biological select agents and toxins that are used for clinical treatment or medical research; and the open nature of these facilities presents a potential security vulnerability. These agents and materials may provide an attractive target to those wishing to construct a "dirty bomb," intentionally infect a population, or sell the material on the black market.
  - Medical systems and vital records are also at risk for compromise or theft by external hackers or malicious insiders, and cybertheft presents a trend in medical identity theft.
- **Pandemic**
  - Recent experience with influenza demonstrated how a rapidly-spreading infectious agent can significantly impact the HPH Sector and the country as a whole. A naturally occurring agent like influenza was able to cause death, hospitalizations, and absenteeism.
  - If a more dangerous agent, such as smallpox, were intentionally released, the effects could be even more catastrophic due to the increased lethality and our general immunological naiveté to the disease.

For More Information

- Sector-Specific Agency: Department of Health and Human Services (HHS), Public Health Preparedness and Emergency, www.phe.gov
- DHS, HHS, *2010 Healthcare and Public Health Sector-Specific Plan*, www.dhs.gov/files/programs/gc_1179866197607.shtm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies and Interdependencies of the Healthcare and Public Health Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Information Technology Sector Sector Risk Snapshot

Critical IT Sector Functions

- IT products and services
- Incident management capabilities
- Domain name resolution services
- Identity management and associated trust support services
- Internet-based content, information, and communications services
- Interrouting, access, and connection services

Information Technology Sector Overview

- Businesses, governments, academia, and private citizens are increasingly dependent upon IT Sector functions. The Information Technology (IT) Sector is central to the Nation's security, economy, public health, and safety.
- These virtual and distributed functions produce and provide hardware, software, IT systems and services, and—in collaboration with the Communications Sector—the Internet.
- The Sector's complex and dynamic environment makes identifying threats and assessing vulnerabilities difficult, and requires that these tasks be addressed in a collaborative and creative fashion.
- The IT Sector functions are operated by a collaboration of entities—often owners and operators and their respective associations—that maintain and reconstitute the network, including the Internet.
- Although the IT infrastructure has a certain level of inherent resilience, its interdependent and interconnected structure presents challenges as well as opportunities for coordinating public and private sector preparedness and protection activities.
- The IT Sector is at constant risk from cyberthreats, and identifying threat actors, intrusion methods, and network vulnerabilities are critical to mitigation and longer-term defensive strategies (Figure 1 and 2).

Figure 1: 2012 Confirmed Data Breach and Network Intrusion Threat Actors

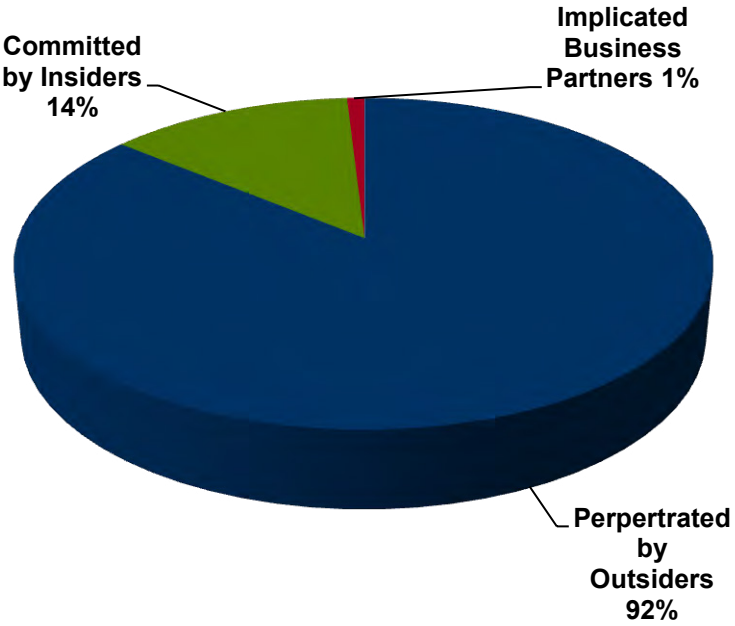
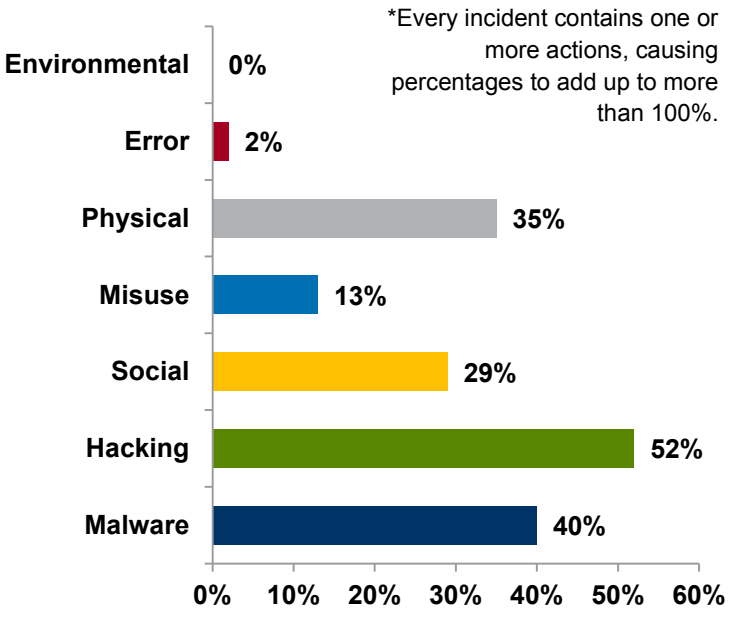


Figure 2: 2012 Confirmed Data Breach and Network Intrusion Threat Actions



Source: Verizon, *2013 Data Breach Investigations Report*, www.verizonenterprise.com/DBIR/2013/

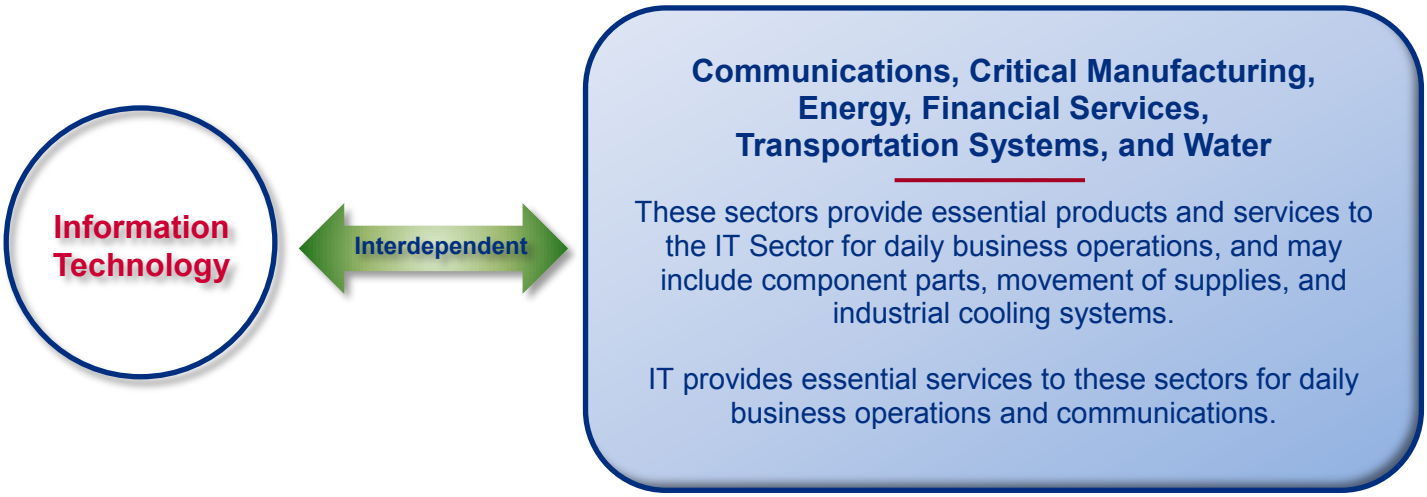
Threats and Hazards of Significant Concern

- **Cyberthreats**
  - The IT Sector is highly concerned about cyberthreats, particularly those that degrade the confidentiality, integrity, or availability of the Sector's critical functions.
  - Depending on its scale, a cyberattack could be debilitating to the IT Sector's highly interdependent critical infrastructures and ultimately to the Nation's economy, homeland security, and national security.
  - These cyberthreats include unintentional acts (e.g., the accidental disruption of Internet content services) and intentional acts (e.g., the exploitation of IT supply chain vulnerabilities or the loss of interoperability between systems as the result of an attack).
- **Attacks Targeting Internet-based Identity**
  - These include attacks targeting management, content, information, and communications. For example, malicious code increasingly proliferates through social networking and can degrade information technology system functionality.
  - Failures in identity management systems can lead to serious consequences like identity theft, criminal activity, unauthorized access to sensitive or classified information, systems, and facilities, which could jeopardize public safety and the operation of financial, government, or law enforcement systems.

For More Information

- Sector-Specific Agency: DHS, Office of Cybersecurity and Communications, www.dhs.gov/office-cybersecurity-and-communications
- DHS IT Sector, www.dhs.gov/information-technology-sector
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- U.S. Cyber Emergency Readiness Team, www.us-cert.gov
- U.S. Industrial Control Systems Cyber Emergency response Team (ICS-CERT), ics-cert.us-cert.gov
- National Vulnerability Database, http://nvd.nist.gov
- FBI Cyber Crime Investigations, www.fbi.gov/about-us/investigate/cyber

Figure 3: Common, First-order Interdependencies of the IT Sector



May 2014

Homeland Security

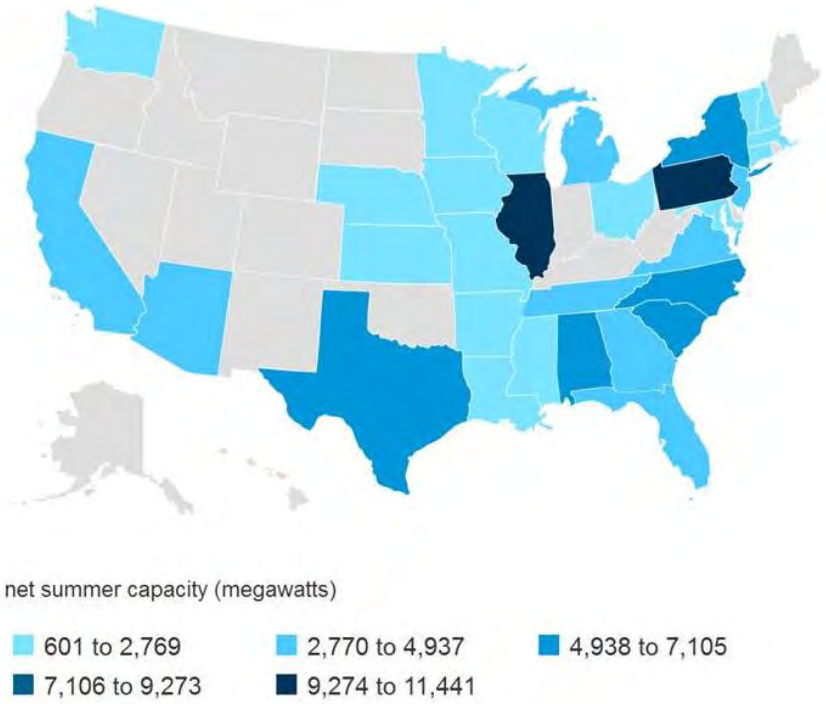
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Nuclear Reactors, Materials, & Waste Sector

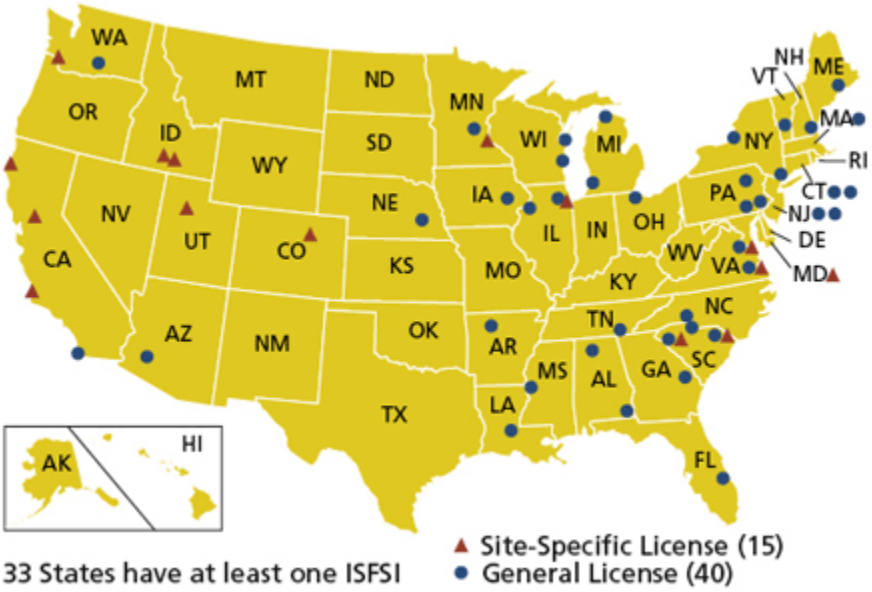
Sector Risk Snapshot

Figure 1: U.S. Nuclear Capacity and Generation



Source: U.S. Energy Information Administration (EIA), *Nuclear and Uranium*, 2014, www.eia.gov/nuclear/state.

Figure 2: Licensed/Operating Independent Spent Fuel Storage Installations



Source: U.S. Nuclear Regulatory Commission, *Locations of Independent Spent Fuel Storage Installations,* 2012, www.nrc.gov/waste/spent-fuel-storage/locations.html.

Nuclear Sector Overview

- Comprises nuclear power plants; research and test reactors; fuel cycle facilities; radioactive waste management; decommissioning reactors; nuclear and radioactive materials used in medical, industrial, and academic settings; and nuclear material transport.
- 104 nuclear power reactors at 65 nuclear power plants account for nearly 20 percent of annual U.S. electricity production (Figure 1). Increases in nuclear generation have roughly tracked the growth in total electricity output.
- There are 31 research and test reactors nationwide. Also known as non-power reactors, they are used primarily for education and research and development.
- Radioactive materials, including more than 75,000 high-activity sources, are used daily in a range of industrial, medical, and other commercial settings.
- The Sector faces current and ongoing risk for Sector facilities and materials due to physical incidents, cyber-disruptions, theft, diversion of materials, and disruptions in the supply chain.
- Theft or diversion of nuclear materials would pose a significant risk to populations through mishandling of the material or the use of a radiological dispersal device (RDD) or, in the worst case, the detonation of an improvised nuclear device.
- If successfully attacked or disrupted, some nuclear facilities have the potential to release radioactive material into the environment.

Radioactive Waste

- Most spent nuclear fuel is safely stored in specially designed pools at individual reactor sites around the country (Figure 2).
- Licensees may move spent fuel rods to above-ground dry storage casks after a minimum 5-year decay period, and if the licensee has an approved above-ground dry storage facility.

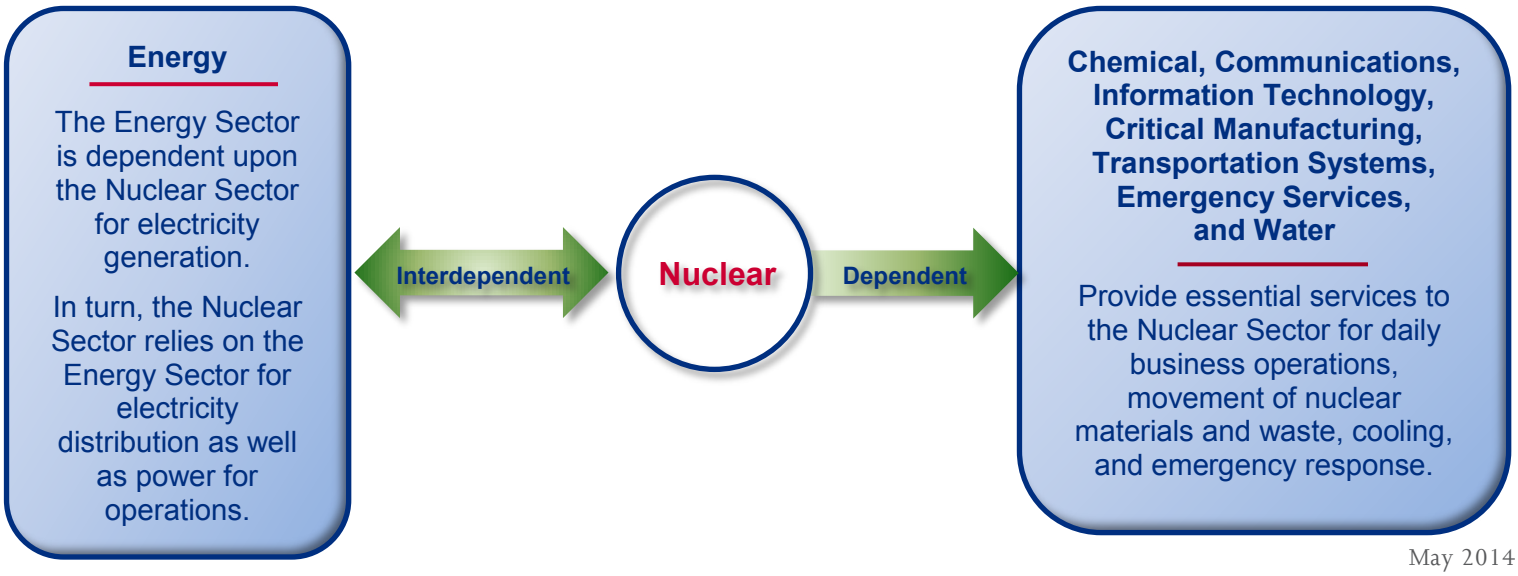
Threats and Hazards of Significant Concern

- **Theft and diversion of nuclear and radioactive materials:**
  - Determined and skilled adversaries could use stolen radioactive materials as elements of improvised nuclear devices (IND), radiological dispersion devices (RDD), or radiological exposure devices.
- **Natural hazards (e.g. hurricanes, tornados, floods, earthquakes, and drought):**
  - Pose a serious and continuing risk for the Sector.
  - The loss or disruption of a single nuclear power plant would have limited impact on the Nation's overall electrical capacity.
  - Sector infrastructure may be severely disrupted or destroyed by such hazards, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies (Figure 3).
- **Physical and cyberattacks on Nuclear Sector infrastructure and assets by terrorists, homegrown extremists, or disgruntled insiders:**
  - Physical attacks using improvised explosive devices on nuclear power reactors, spent fuel and radioactive waste storage facilities, and fuel cycle facilities could result in a release of hazardous materials.
  - Cyberattacks and intrusions on industrial control systems may pose a significant threat to the Sector, allowing malicious actors to manipulate or exploit facility operations.

For More Information

- Sector-Specific Agency: DHS, Office of Infrastructure Protection, www.dhs.gov/about-office-infrastructure-protection
- Nuclear Regulatory Commission, www.NRC.gov
- Nuclear Energy Institute, www.NEI.org
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS, 2010 Nuclear Reactors, Materials, and Waste Sector-Specific Plan, www.dhs.gov/files/programs/gc_1179866197607.shtm

Figure 3: Common, First-order Dependencies and Interdependencies of the Nuclear Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Aviation Mode
Transportation Sector

Sector Risk Snapshot

Figure 1: Major Continental U.S. Airport Locations

Table 1: Schedules System (Domestic and International) Airline Travel on U.S. Airlines

	2012	2013	Change %
Passengers (in millions)	736.7	743.1	0.9
Flights (in thousands)	9,287.40	7,158.70	-1.4
Revenue Passenger Miles (in billions)	823.2	840.4	2.1
Available Seat-miles (in billions)	994.5	1.011.20	1.7
Load Factor*	82.8	83.1	0.3
Flight Stage Length**	755	770.3	2
Passenger Trip Length***	1,117.40	1,131.00	1.2

Source: Bureau of Transportation Statistics, *T-100 Market and Segment*, March 13, 2014, www.rita.dot.gov/bts/press_releases/bts012_14
* Measure of the amount of utilization of the total available capacity of an airline, i.e. percent of available seat-miles (ASM) occupied by passengers
** The average non-stop distance flown per departure in miles
*** The average distance flown per passenger in miles
Note: Percentage changes based on numbers prior to rounding.

Aviation Mode Overview

- The Aviation Transportation System (ATS) is a vital mode within the Transportation Sector, integrally contributing to the free flow of people and commerce across the globe.
- The Aviation Mode consists of more than 19,700 airports in the United States. Of these, 5,170 are open to the general public with 503 offering commercial service.
- The ATS includes more than 690 air traffic control facilities, and over 11,000 air navigation facilities.
- More than 780,000 passenger flights take place over the United States each month carrying nearly 60 million passengers.
- This Mode transports more than 13 million ton-miles of freight domestically each year.
- The security and economic prosperity of the United States depend significantly upon the secure operation of its ATS and safe use of the world's airspace.
- Significant threats to the ATS include the potential for terrorist infiltrations and attacks, cyber attacks against ATS assets, and the hostile exploitation of air cargo.
- The U.S. Department of Homeland Security (DHS), Department of Transportation (DOT), and Department of Defense (DOD) continue to develop and enhance technological and procedural measures to detect, prevent, respond to, mitigate and recover from physical and cyber-based attacks on the ATS's critical infrastructure.

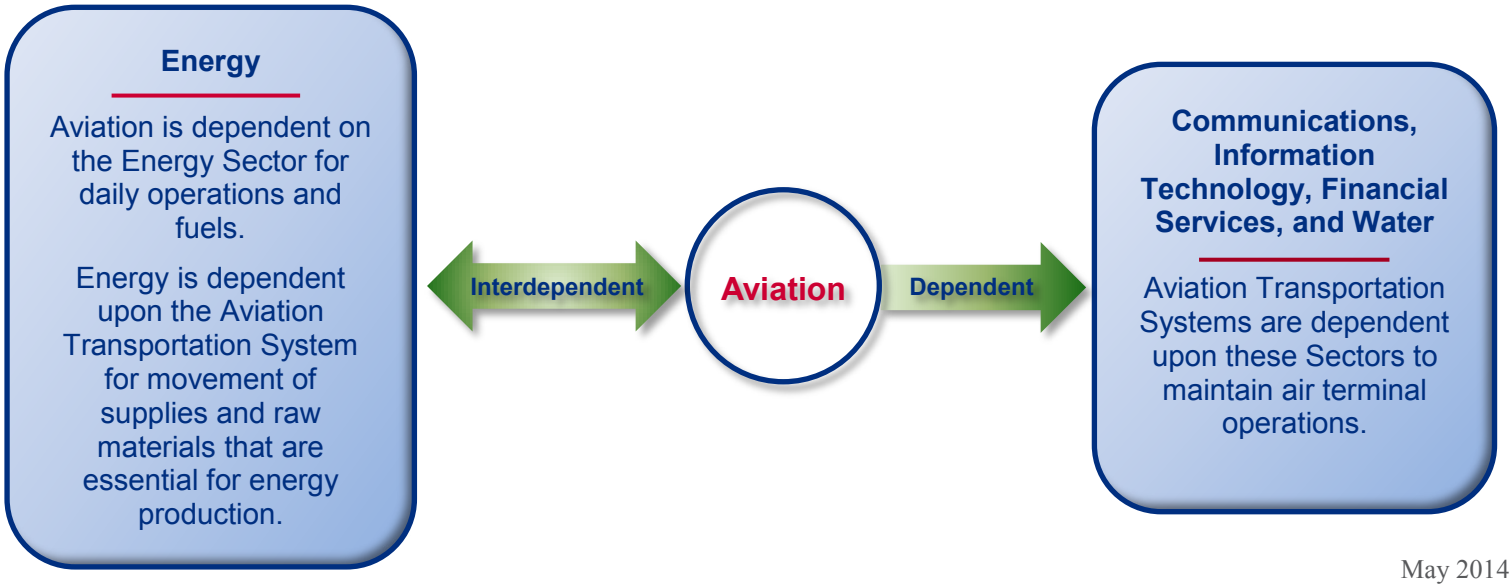
Threats and Hazards of Significant Concern

- **Terrorism**
  - Terrorism threats to the ATS persist. Aircraft have been the primary target of attacks in the past, and have been used as weapons. Despite security enhancements made after the attacks on September 11, 2001, intelligence continues to indicate that aviation remains a top target of terrorists. (DHS and TSA, 2011)
  - Terrorist groups are adapting to aviation countermeasures in multiple ways, including modality of planning, complexity of potential attacks, and methods of attack execution.
- **Cyberthreats**
  - The Sector focuses on developing countermeasures to address specific risks in the cyber-realm. A concerted, well-orchestrated attack on any Sector cybernetwork could cause considerable disruption Sector-wide.
  - The Federal Aviation Administration is collaborating with industry, academia, and other Federal agencies on aircraft cybersecurity research and development *(https://faaco.faa.gov/index.cfm/announcement/view/14453)*.
- **Cargo**
  - The air-cargo industry is highly dynamic and encompasses a wide range of users, characteristics which expose it to exploitation by terrorists.
  - Terrorists may use unsecured air transportation routes to transport arms, explosives, or operatives clandestinely to safe havens, training sites, or attack-staging locations. Ultimately, terrorists may use these access points and routes to transport more dangerous cargo, including weapons of mass destruction and their associated components.

For More Information

- Sector-Specific Agency: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- Federal Aviation Administration, www.faa.gov
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 2: Common, First-order Dependencies and Interdependencies of the Aviation Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Freight Rail Mode
Transportation Sector

Sector Risk Snapshot

Figure 1: The rail network accounts for approximately 40 percent of U.S. freight moves by ton-miles (the length freight travels)
Source: Federal Railroad Administration, "National Rail Plan Progress Report," 2010

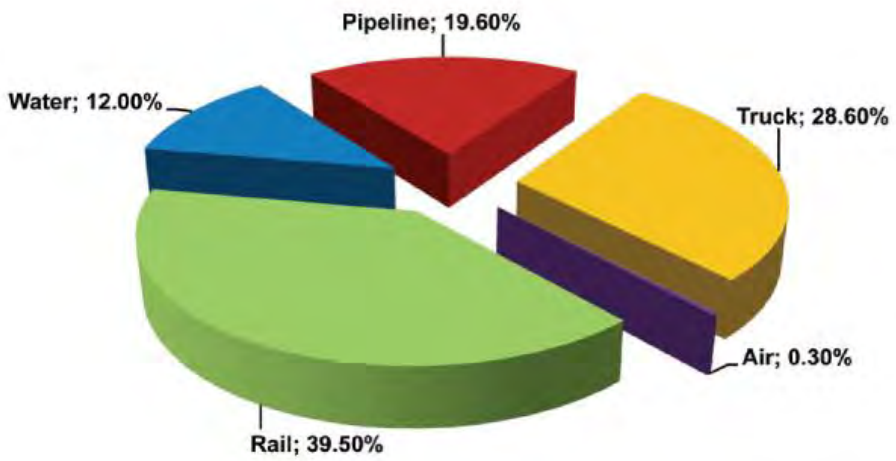
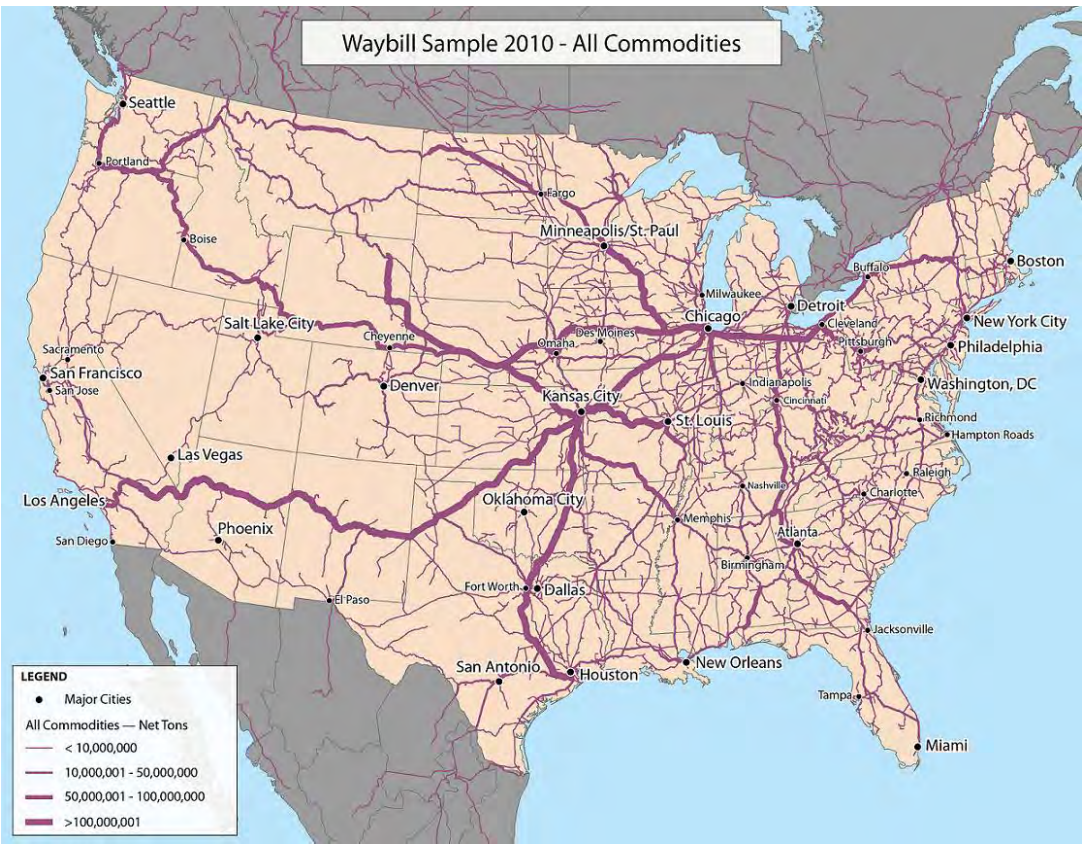


Figure 2: U.S. Freight Rail System Map
Source: Federal Railroad Administration, based on Surface Transportation Board's 2010 Carload Waybill Sample



Freight Rail Mode Overview

- **Freight Rail is one of seven modes that make up the Transportation Sector.**
- **The $60 billion industry consists of 140,000 miles of active rail track and provides 221,000 jobs across the country.**
- **Passenger and commuter rail systems throughout the country operate at least partially over tracks or rights-of-way owned by freight railroads. The National Railroad Passenger Corporation (Amtrak), for example, operates on more than 22,000 miles of track owned by freight railroads.**
- **Freight rail comprises 565 carriers divided among 3 Classes: Class I are the 7 major long haul carriers responsible for approximately 93 percent of total Sector revenue; the remaining 558 carriers (Class II and III) are local or short-haul carriers.**
- **Freight rail plays a critical role in support of the Energy Sector. Freight railroads are responsible for the transportation of more than 70 percent of all U.S. coal shipments (7.0 million carloads in 2010). Coal is the fuel that generates half of America's electricity.**

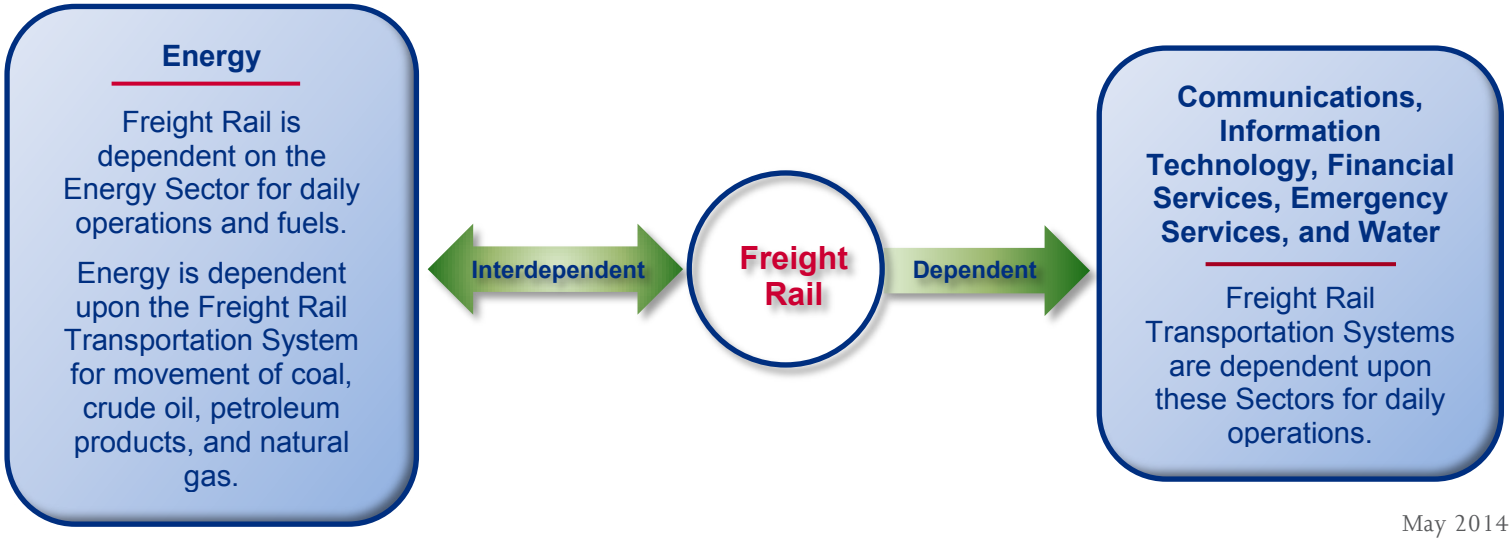
Threats and Hazards of Significant Concern

- **Sensitive Freight and Access Points**
  - Transportation Security Administration's (TSA's) risk assessment efforts examine the critical assets (e.g., bridges, tunnels, and yards) required for carrying out the freight railroad's basic mission of moving freight. Rail yards and terminals represent the fixed points in the network of railroad assets at which cars are transferred from one train to another, inspected, and repaired as necessary.
  - The movements of security-sensitive materials and toxic inhalation hazard materials through freight rail facilities, or over open tracks, leave railroad employees and public populations vulnerable if confronted with the threat of a terrorist attack.
- **Terrorist Attacks**
  - Intelligence reviews of various attacks worldwide, as well as analysis of seized documents, and the interrogation of captured and arrested suspects, reveal that there has been historic interest in carrying out attacks on railroad systems, particularly passenger rail systems due to the potential for large civilian casualties.
  - TSA concludes that long stretches of open, unattended track and numerous critical points (e.g., junctions, bridges, contiguous passenger rail sites) that are difficult to secure make the U.S. freight rail system an attractive target for terrorist attacks.
- **Insider Threat**
  - While the risk is considered low to moderate, documented evidence shows that disgruntled persons have tampered with tracks and other rail components.
  - Control systems are also vulnerable to tampering or external cyberattacks. However, the fail-safe nature of freight rail control systems may serve to mitigate the risk of a catastrophic incident.

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- Federal Rail Administration, www.fra.dot.gov
- American Association of Railroads, www.aar.org
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, 2010 Transportation Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 3: Common, First-order Dependencies and Interdependencies of the Freight Rail Mode



May 2014

Homeland Security

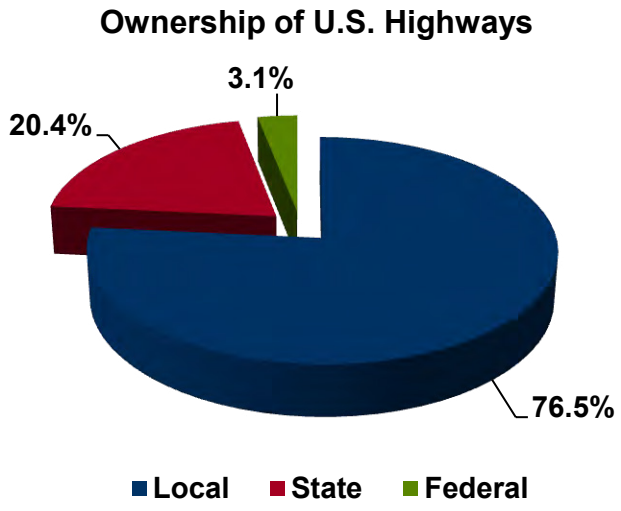
Highway and Motor Carrier Mode
Transportation Sector

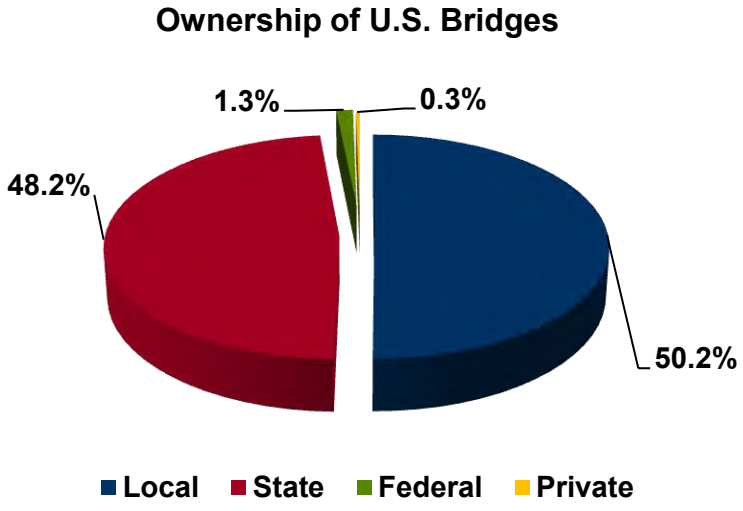
Sector Risk Snapshot

Highway and Motor Carrier Mode Overview

- **The Highway & Motor Carrier Mode assets include, but are not limited to, bridges, major tunnels, operations and management centers, trucks carrying hazardous materials, other commercial freight vehicles, motor coaches, school buses, and key intermodal facilities.**
- **The trucking industry is unique in that it is the only segment of the Highway Mode with complete intermodal supply chain relationships with aviation, maritime, mass transit, freight rail, and pipeline.**
- **The Nation's highway network includes nearly 4 million miles of roadway, almost 600,000 bridges, and some 400 tunnels.**
- **This Mode faces current and ongoing risk to facilities and materials due to terrorist attacks, natural hazards, and cyber-incidents.**
- **If successfully attacked or disrupted, impacts could result in regional shutdowns, diversions, or costly repairs with potentially severe results.**

Figure 1: Ownership of U.S. Highways and Bridges (2010)
Source: Department of Transportation, Federal Highway Administration, 2013 *Status of the Nation's Highways, Bridges, and Transit: Conditions & Performance*, January 31, 2014, www.fhwa.dot.gov/policy/2013cpr/overviews.htm





Hazardous Materials

- **The Transportation Security Administration (TSA) Hazardous Materials Endorsement Threat Assessment Program conducts a security threat assessment for any driver seeking to obtain, renew, or transfer a hazardous materials endorsement on a state-issued commercial driver's license.**
- **Hazardous materials include poisonous vapors, aerosols, liquids, and solids that have toxic effects on people, animals, or plants.**
- **They can have an immediate effect (a few seconds to a few minutes) or a delayed effect (2 to 48 hours).**
- **While potentially lethal, chemical agents are difficult to deliver in lethal concentrations. Outdoors, the agents often dissipate rapidly.**

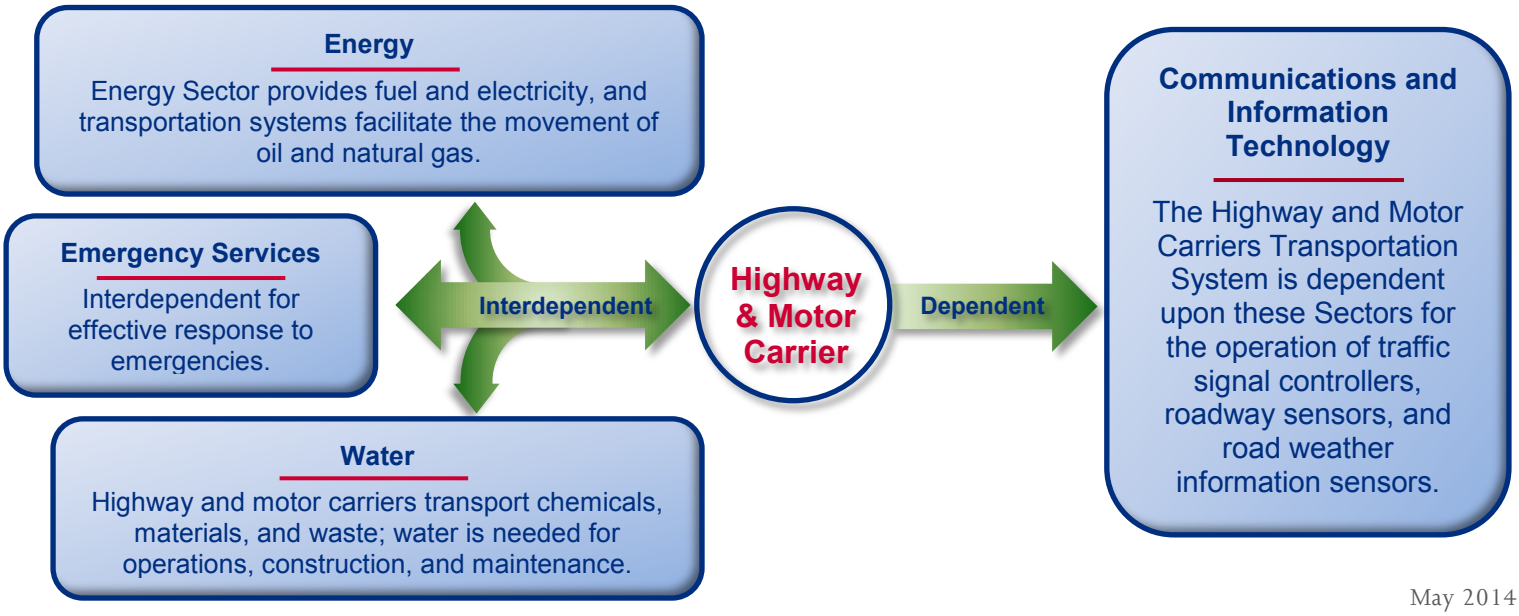
Threats and Hazards of Significant Concern

- **Terrorist attacks involving highway infrastructure and assets**
  - Highway infrastructure and assets may either be a target [e.g., improvised explosive devices (IEDs) against highway structures] or serves as a means to conduct an attack against other targets (e.g. use of a truck as a vehicle-borne IED against a building).
  - Use of HAZMAT materials as a terrorist attack is a serious and continuing risk to the Highway Mode.
- **Natural hazards, such as hurricanes, tornadoes, floods, and earthquakes**
  - Highway infrastructure may be severely disrupted or destroyed by such hazards, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies.
- **Cyberattacks on highway infrastructure by terrorists, homegrown extremists, or disgruntled insiders**
  - Cyberattacks and intrusions on traffic control systems or other business systems pose a serious threat to highway infrastructure allowing malicious actors to manipulate or exploit control systems essential to operation of traffic control systems and highway messaging systems.

For More Information

- Sector-Specific Agency: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- American Association of State Highway and Transportation Officials, http://transportation.org/default.html
- American Bus Association, www.buses.org
- American Trucking Association, www.trucking.org/Pages/Home.aspx
- Federal Highway Administration, www.fhwa.dot.gov
- Pipeline and Hazardous Materials Safety Administration, http://phmsa.dot.gov/hazmat
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 2: Common, First-order Dependencies and Interdependencies of the Highway and Motor Carrier Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Maritime Mode
Transportation Sector

Sector Risk Snapshot

Figure 1: U.S. Import Value by Mode of Transportation, 2011, in Millions of U.S. Dollars

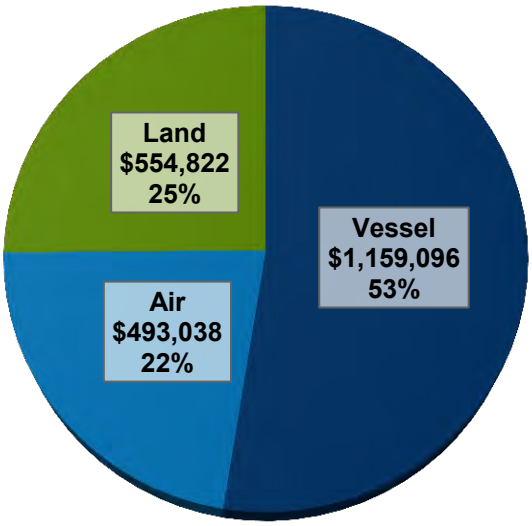
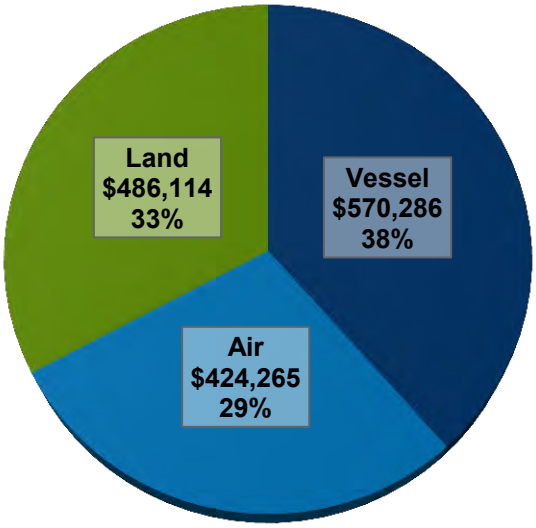


Figure 2: U.S. Export Value by Mode of Transportation, 2011, in Millions of U.S. Dollars



SOURCE Figures 1-2: U.S. Department of Transportation, Bureau of Transportation Statistics, "Maritime Trade and Transportation by the Numbers," accessed December 2013,www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/by_the_numbers/maritime_trade_and_transportation/index.html

Maritime Mode Overview

- **Maritime is one of seven modes that make up the Transportation Systems Sector.**
- **The Marine Transportation System (MTS) is a geographically and physically complex and diverse system consisting of waterways, ports, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from, and on the water.**
- **The Mode consists of nearly 95,000 miles of coastline, 361 ports, over 25,000 miles of navigable waterways, over 29,000 miles of Marine Highway and 3.4 million square miles of Exclusive Economic Zone.**
- **The Exclusive Economic Zone is the area where the U.S. has jurisdiction over economic and resource management. U.S. Marine Highways are navigable waterways that have been designated by the Secretary of Transportation and have demonstrated the ability to provide additional capacity to relieve congested landside routes serving freight and passenger movement.**
- **Ships plying the maritime domain are the primary mode of transportation for global trade, carrying more than 80 percent of the world's trade by volume.**
- **In addition to the movement of freight, the marine transportation system serves as a critical component of the Nation's passenger transportation network. Over 200 ferry operators provide safe and reliable transportation for passengers and vehicles, while cruise ships and recreational boats contribute billions to the U.S. economy.**
- **The Mode faces current and ongoing risk for Sector facilities and materials due to potential cyberintrusion, port vulnerability, and insecure intermodal shoreside connections.**

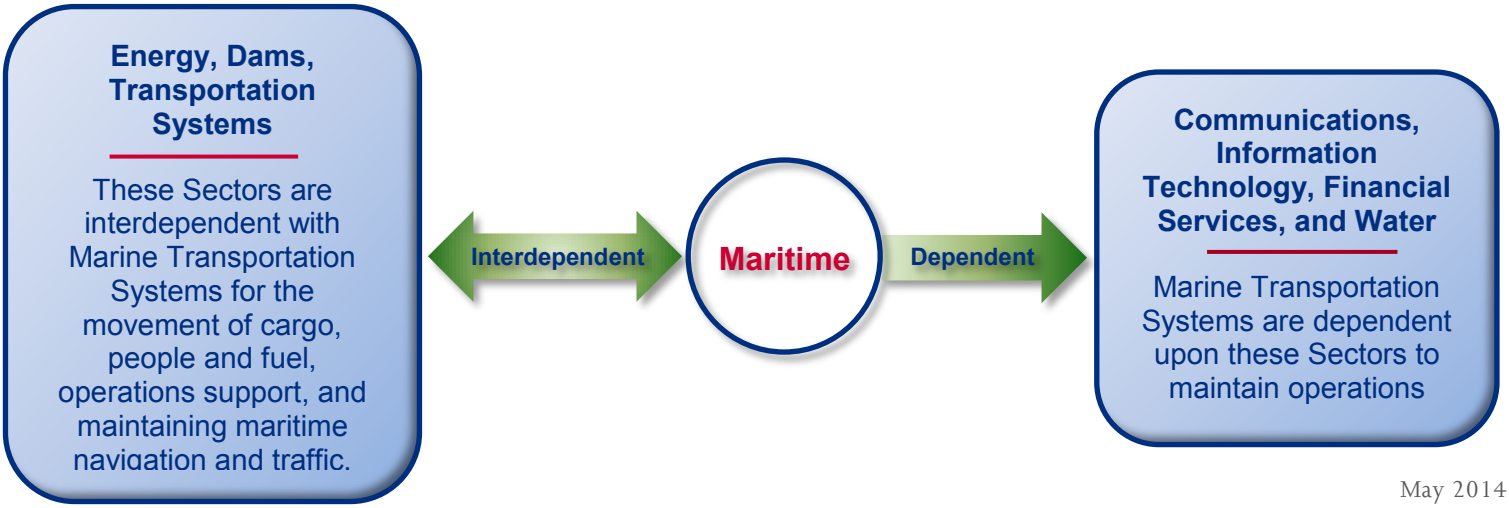
Threats and Hazards of Significant Concern

- **Natural Disasters**
  - From a risk-based perspective, the greatest risk facing the U.S. maritime domain, based on likelihood and consequence, is a major natural disaster, particularly hurricanes, flooding, drought, and tsunami.
  - These events are known to occur frequently and their consequences are often severe.
- **Cybersecurity**
  - Has become more important as the MTS has become increasingly dependent on cybersystems and faces a growing threat from cyberattacks.
  - These systems are used for a variety of purposes, including access control, navigation, traffic monitoring, and information transmission. Although the interconnectivity and utilization of cybersystems facilitate transport, they can also present opportunities for exploitation, contributing to risk for the MTS.
- **Malicious Actors**
  - Even though a robust security planning system (which includes ports, domestic facilities and vessels, as well as foreign vessels that call into the United States) has been implemented through the Maritime Transportation Security Act, a successful attack on critical infrastructure or nodes could cause transportation disruptions with cascading effects.
  - Port facilities and the ships and barges that transit port waterways are also somewhat vulnerable to tampering, theft, and unauthorized persons gaining entry to collect information and commit unlawful or hostile acts. Because of just-in-time method use, a successful attack against one node of maritime infrastructure could disrupt entire systems, cause congestion, limit capacity for product delivery, significantly damage the economy, or create an inability to project military force. Risks related to small vessel security also continue to be a focus of the U.S. Coast Guard (USCG).
- **"Dark Targets"**
  - Numerous maritime security assessments, most notably the DHS Small Vessel Security Strategy and the Current State Report of the Maritime Domain Awareness Interagency Solutions Analysis, have concluded that small "dark targets"—smaller vessels that are not required to carry electronic identification devices, make advance notices of arrival, or otherwise alert authorities to their whereabouts—constitute a major maritime awareness gap.
  - Although the majority of dark targets are legitimate, illicit operators can take advantage of their being difficult to detect and smuggle illegal cargo or people, or serve as waterborne platforms for terrorism.

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), http://www.tsa.gov, USCG, www.uscg.mil
- U.S. Department of Transportation, Maritime Administration, www.marad.dot.gov
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, 2010 Transportation Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 3: Common, First-order Dependencies and Interdependencies of the Maritime Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Mass Transit Mode
Transportation Sector

Sector Risk Snapshot

Table 1: U.S. Unlinked Passenger Trips by Mode Report Year 2011

Mode of Service	Passenger Trips	
	Millions	Percent
Bus	5,191	50.3
Bus Rapid Transit	6	0.1
Commuter Bus	37	0.4
Commuter Rail	466	4.5
Demand Response	191	1.9
Ferryboat	80	0.8
Heavy Rail	3,647	35.3
Hybrid Rail	6	0.1
Light Rail	436	4.2
Other Rail Modes*	44	0.4
Publico†	39	0.4
Streetcar	43	0.4
Transit Vanpool	34	0.3
Trolleybus	98	0.9
Total All Modes	10,319	100

*Aerial Tramway, automated guideway transit, cable car, inclined plane, and monorail.
†Publico is a mode of transit service provided by small vans or buses operated in San Juan, PR

Figure 1: Since 2004, Transit Use has Grown More Than Population or Highway Travel

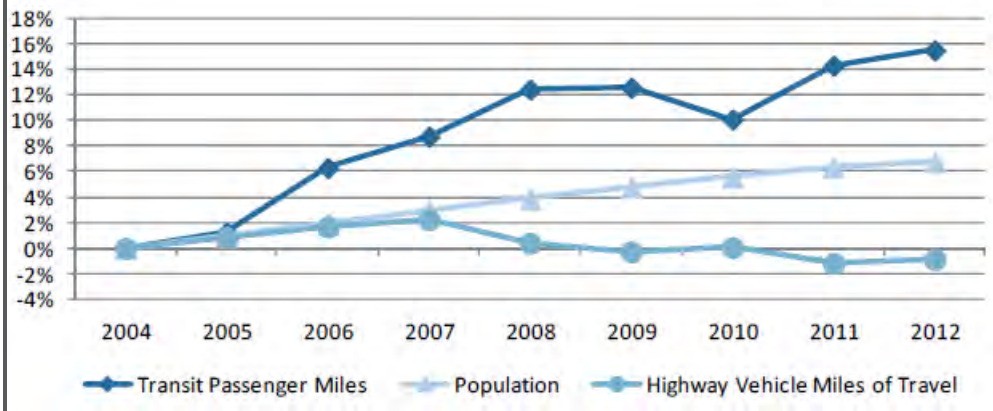


Table 1 and Figure 1 Source: American Public Transportation Association, "2013 Public Transportation Fact Book," Accessed December 2013, www.apta.com/resources/statistics/Pages/transitstats.aspx

Mass Transit Mode Overview

- **The Mass Transit and Passenger Rail Mode includes service by buses, rail transit (commuter rail, heavy rail, also known as subways, and light rail, including trolleys and streetcars), long-distance rail (namely Amtrak and Alaska Railroad), and other, less common types of service. It also includes demand response services for seniors and persons with disabilities, as well as vanpool/rideshare programs and taxi services operated under contract with a public transportation agency. The Mass Transit Mode does not include over-the-road motor coach operators, school bus systems, or private shuttle system operators.**
- **Passengers take 35 million trips each weekday in the United States. As part of an intermodal system of transportation, the Mass Transit Mode also connects to other modes of transportation through multimodal systems and within multimodal infrastructures.**
- **In 2011, U.S. public transportation was provided by 7,100 organizations, ranging from large multimodal systems to single-vehicle special demand response providers.**
- **In 2011, public transportation agencies spent $55 billion for operation of service and capital investment.**
- **The yearly totals for 2011 show that passengers took 10.3 billion trips and rode transit vehicles for 56.1 billion miles.**
- **The Mass Transit Mode includes thousands of employees, operational and maintenance facilities, construction sites, utilities, administrative facilities, and thousands of computerized networks, which facilitate operations and ensure efficient and reliable service.**

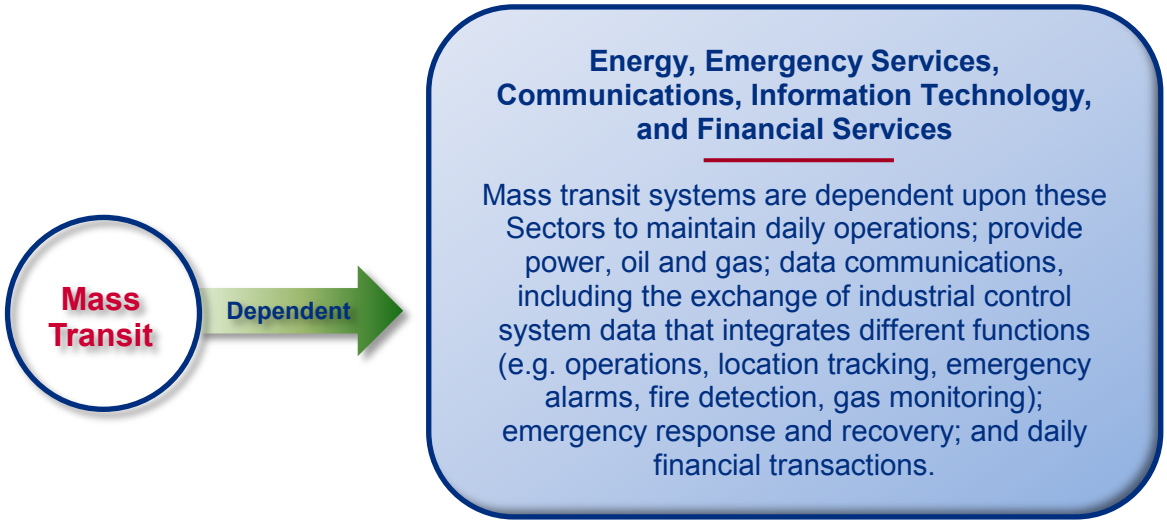
Threats and Hazards of Significant Concern

- **Access**
  - Unlike air transport, where strict access controls and universal security screening apply, public transportation operates more openly, in fast-paced operations with numerous entry, transfer, and exit points, to transport a high volume of passengers every day that greatly exceeds the number of air travelers. Multiple stops and interchanges lead to high passenger turnover, which is difficult to monitor effectively.
  - Broad geographical coverage of mass transit and passenger rail networks provide numerous options for access and getaway and afford the ability to use the system itself as the means to reach the location to conduct the attack.
- **Physical Attacks**
  - Physical attacks on the Mass Transit Mode represents a significant risk to the Sector, and may include a vehicle bomb near a station or track, explosives on a track, release of a caustic or biological agent in an enclosed station, tampering with rail switches, or an improvised explosive device or a lower-yield explosive in a station, train, or bus. Physical attacks on the Mass Transit Mode have to chance to result in scores of casualties. Consequences of such attacks can result in severe economic disruption and can impact the continuity of government operations.
- **Terrorism**
  - Attacks on mass transit systems are an attractive target for terrorists, and can result in a large number of victims, both killed and wounded, significant property damage, and loss of public confidence in public transit systems and Federal, State, local, and tribal governments. Coordinated attacks that simultaneously target multiple nodes in the system can potentially disrupt city-wide public transit operations, increasing public confusion and panic.
  - Examples of coordinated terrorist attacks on the Mass Transit Mode include the 1995 release of sarin gas in the Tokyo subway, which killed 13 people, severely injured 50, and caused temporary vision problems in over a 1000 others, and the 2005 bombings in London, in which IEDs were detonated in three London Underground trains across the city and a double-decker bus. The London bombings resulted in the deaths of 52 civilians and over 700 casualties.

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov and Department of Transportation, www.dot.gov
- American Public Transportation Association, www.apta.com
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Figure 2: Common, First-order Dependencies of the Mass Transit Mode



May 2014

Homeland Security

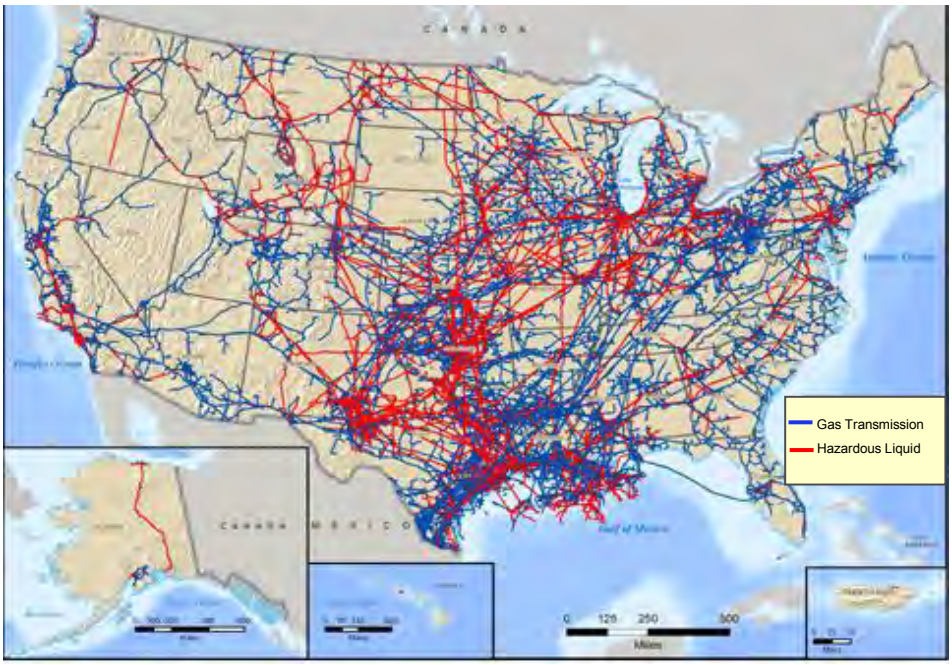
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Pipeline Mode
Transportation Sector

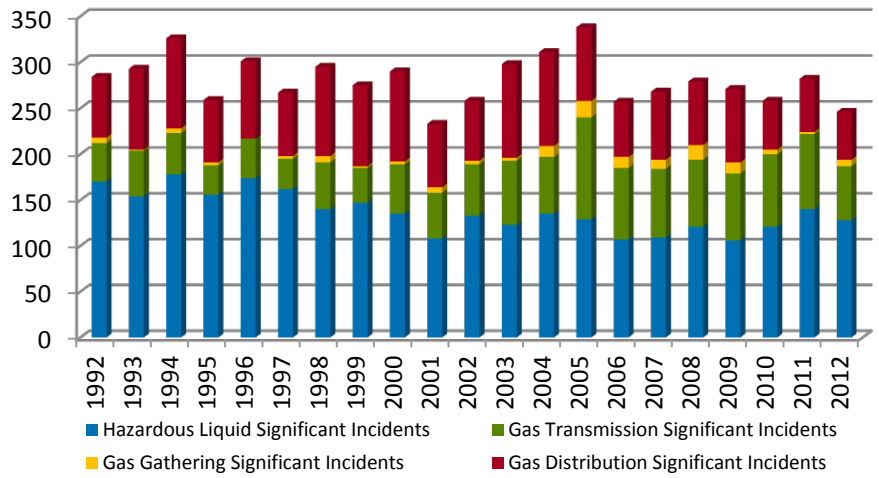
Sector Risk Snapshot

Figure 1: U.S. Gas Transmission and Hazardous Liquid Pipelines



Source: U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration (PHMSA), National Pipeline Mapping System, March 2012.

Figure 2: Number of Significant Pipeline Systems Incidents 1992-2012*



*Significant Incidents are those incidents reported by pipeline operators when any of the following specifically defined consequences occur: 1) fatality or injury requiring in-patient hospitalization; (2) $50,000 or more in total costs; (3) highly volatile liquid releases of 5 barrels or more; or, (4) other liquid releases of 50 barrels or more resulting in an unintentional fire or explosion.

Source: PHMSA, *Significant Pipeline Incidents*, http://primis.phmsa.dot.gov/comm/reports/safety/sigpsi.html

Pipeline Mode Overview

- Pipelines are one of seven modes that make up the Transportation Sector.
- More than 2.5 million miles of pipelines network the United States to transport nearly all of the natural gas and about 65 percent of hazardous liquids, including crude and refined petroleum products, consumed within the United States.
- There are four main types of pipelines, most of which are buried underground: 1) Natural Gas Transmission and Storage; 2) Hazardous Liquid Pipelines and Tanks; 3) Natural Gas Distribution; and 4) Liquefied Natural Gas (LNG) Processing and Storage Facilities.
- Cross-border (international) pipelines are becoming increasingly important to the Nation's pipeline industry, which is prompting the U.S. and Canada to conduct joint assessments on trans-border infrastructure and identify necessary additional protective measures.
- While most pipelines are buried, the system has above-ground assets (e.g. wellheads, compressor stations, pumping stations, and processing facilities) that may be vulnerable to attack.
- The Mode faces current and ongoing risk to the movement of pipeline materials via direct attack upon critical pipeline system infrastructure and from cyberattacks against pipeline control systems and networks.

Toxic Inhalation Hazard

- A successful deliberate terrorist attack against toxic inhalation hazard (TIH) materials poses serious risks of fatalities and injuries, especially if the attack were to occur in a highly populated urban area.
- Pipelines are used to transport TIH chemicals such as anhydrous ammonia, a critical fertilizer for the American farming industry and feedstock for the chemical industry.

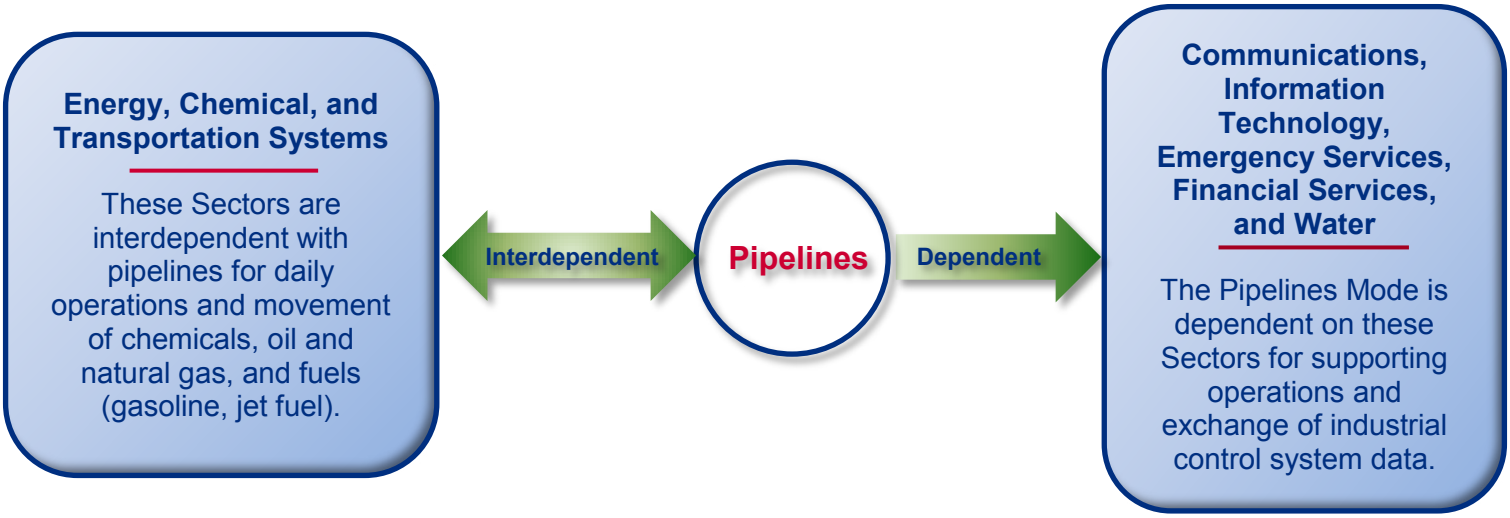
Threats and Hazards of Significant Concern

- **Release of Pipeline Materials**
  - The pipeline system is uniquely vulnerable to terrorist attacks because of the products transported and because pipeline networks are widely dispersed across both remote and urban portions of the country.
  - Many pipelines carry volatile and flammable materials that have the potential to cause serious injury to the public and the environment. A pipeline facility could be vandalized or attacked with explosive devices, resulting in flow disruption or the release of its contents.
- **Cyberthreats**
  - Pipelines are also susceptible to cyberattacks on their computer control systems. Cyberthreats could result from the acts of a terrorist-hacker or a rogue employee with computer access.
  - The latter threat requires that specific attention be given to personnel security credentials and access protocols, as well as general cybersecurity protocols.
- **Cascading Effects from Disruptions to Critical Dependencies**
  - In addition, attacks on other infrastructure, such as regional electricity grids and communication networks, could cause a serious disruption in pipeline operations, posing risks for all Sectors serviced by pipelines, including the military and major commercial installations (Figure 3).

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- Pipeline and Hazardous Materials Safety Administration (PHMSA), www.phmsa.dot.gov
- American Petroleum Institute, www.api.org
- American Gas Association, www.aga.org
- DHS, *National Risk Profile*, OCIA@hq.dhs.gov
- DHS and TSA, *2010 Transportation Sector-Specific Plan*, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf
- Interstate Natural Gas Association of America (INGAA) , www.ingaa.org
- Association of Oil Pipelines (AOPL), www.aopl.org

Figure 3: Common, First-order Dependencies and Interdependencies of the Pipeline Mode



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Postal and Shipping Mode
Transportation Sector

Sector Risk Snapshot

Table 1: Size of the U.S. Mailing Industry

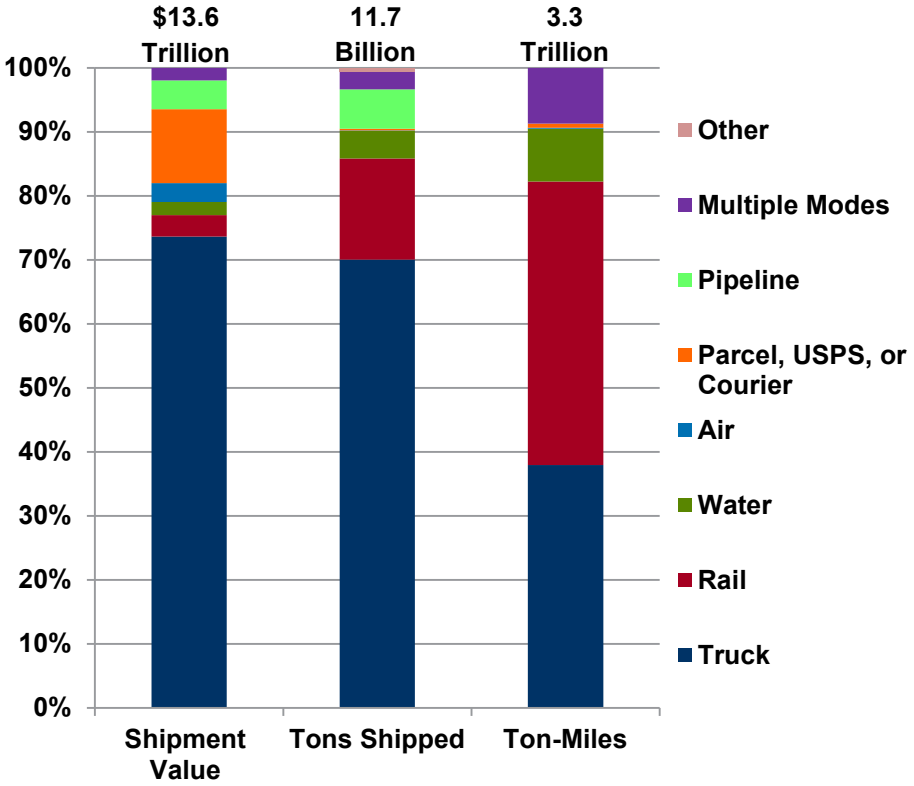
The size of the mailing industry compared to other key U.S. industries is significant. What happens in the mailing industry echoes throughout the economy as it supports over 8.6 percent of the U.S. Gross Domestic Product.

Industry	Number of Jobs Supported	Annual Revenue Supported
Mailing	8.4 million	$1.3 Trillion
Airline	10.0 Million	$1.0 Trillion
Oil and Natural Gas	9.6 million	$1.1 Trillion

SOURCE: U.S. Postal Service, *USPS FY2013 Annual Report to Congress*, 2013.

Figure 1: Value, Tonnage, and Ton-Miles of Shipments by Mode

In 2012, parcel delivery, USPS, and other courier services accounted for 11.6 percent of shipments by value, but less than half of one percent by tonnage, demonstrating that the Postal and Shipping industry typically ships higher value products.



SOURCE: U.S. Department of Transportation, Bureau of Transportation Statistics and U.S. Department of Commerce, U.S. Census Bureau, *2012 Economic Census: Transportation Commodity Flow Survey*, Preliminary Release, December 2013.

Postal and Shipping Mode Overview

- Postal and Shipping is one of seven modes that make up the Transportation Sector.
- Postal and Shipping was formerly recognized as a stand-alone Sector until the February 2013 release of Presidential Policy Directive-21 (PPD-21), when Postal and Shipping was incorporated into the Transportation Sector.
- Composed of large integrated carriers, regional and local courier service providers, mail services and mail management firms, and chartered air delivery services.
- Four large integrated carriers—the U.S. Postal Service (USPS), the United Parcel Service (UPS), FedEx, and DHL International—account for 94 percent of the Mode's assets systems, networks, and functions.
- Postal and Shipping moves more than 720 million messages, products, and financial transactions each day.
- The threat environment to the mode includes attacks on infrastructure, operations, and employees, and the use of the Mode to attack its customers, other Sectors, or the economy as a whole, using targeted or widespread techniques and tactics.
- Mode risk is a function of the vulnerability of an extremely large number of collection points, many of which are open and anonymous.
- The Mode is a highly trusted entity, and its employees and representatives have ready access to businesses and residences throughout the country.
- The Mode faces current and ongoing risk, due to terrorist attacks using hazardous materials, as well as chemical, biological, radiological, and nuclear explosives (CBRNE) for mail-based attacks.

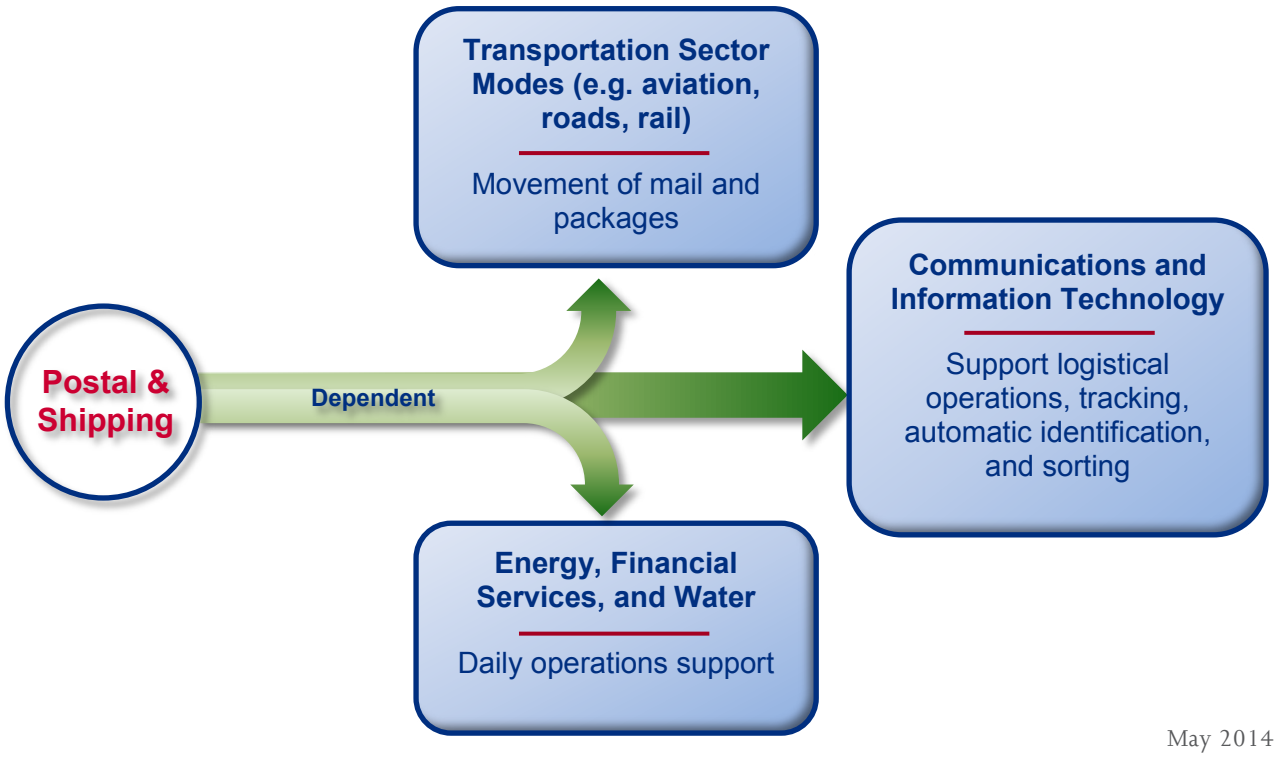
Threats and Hazards of Significant Concern

- **Open Access and Entry Points**
  - By design, the Postal and Shipping Mode is an open system with an extremely large number of entry and collection points, many of which are anonymous. These facilities present a vast number of entry points where dangerous materials could be inserted for delivery to intended targets.
- **Mail-based Threats**
  - Mail-based threats pose a significant and continuing risk for the Postal and Shipping Mode. For example, the Unabomber, Ted Kaczynski, hand-delivered or used the Postal Service over the course of 17 years to deliver parcel bombs that killed three Americans and injured 24 more (FBI, 2008).
  - Physical attacks using improvised explosive devices (letter bombs and parcel-based attacks) against postal and shipping facilities, or against other Sectors, could result in changes in the flow of ground and air mail and delays in mail service.
  - Postal and shipping infrastructure may be severely disrupted by such attacks, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies (Figure 2).
- **Attacks Using Hazardous Materials or CBRNE**
  - The Postal and Shipping Mode is one of the few infrastructures that have been threatened by biological agents; in 2001, the USPS was used as a vehicle for delivering anthrax against multiple targets.
  - In 2010, the terrorist organization Al-Qaeda in the Arabian Peninsula (AQAP) planted bombs in two packages of printer cartridges found on separate cargo planes. Both U.S. and U.K. intelligence officials speculated that the bombs were probably designed to detonate mid-air, with the intention of destroying both planes over Chicago or another city in the U.S. (BBC, 2010, www.bbc.co.uk/news/world-us-canada-11671377)

For More Information

- Sector-Specific Agencies: DHS, Transportation Security Administration (TSA), www.tsa.gov, Department of Transportation, www.dot.gov
- USPS, www.usps.com and http://about.usps.com/securing-the-mail/mail-security-center.htm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 2: Common, First-order Dependencies of the Postal and Shipping Mode



May 2014

Homeland Security

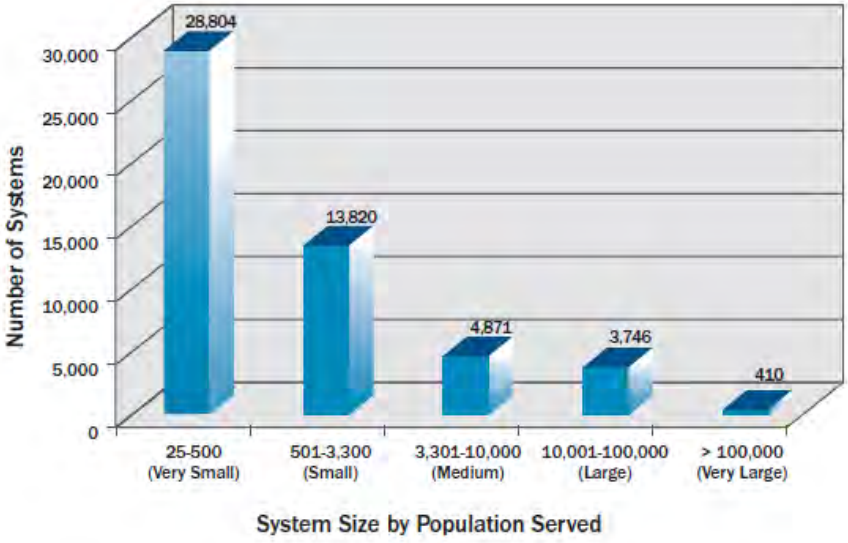
Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

Homeland Security

Water and Wastewater Systems Sector

Sector Risk Snapshot

Figure 1: Community Drinking Water Systems and System Size.
Source: EPA, Safe Drinking Water Information System (SDWIS)



Drinking Water

- A drinking water contamination incident or the denial of drinking water services would have far-reaching public health, economic, environmental, and psychological impacts across the Nation.
- Other critical services, such as fire protection, healthcare, and heating and cooling processes, would also be disrupted by the interruption or cessation of drinking water service, resulting in significant consequences to the national or regional economies.
- The majority of community water systems (CWS) are small systems that serve approximately 8 percent of the population who get their water from CWS (Figure 1).
- Only 17 percent of CWS are classified as medium or large systems, but these systems serve the majority of the U.S. population.
- The EPA reports that CWS served 300.2 million people, while non-community water systems (e.g. schools, factories, hospitals, campgrounds, and gas stations that have their own water systems) served 19.5 million people in 2010.

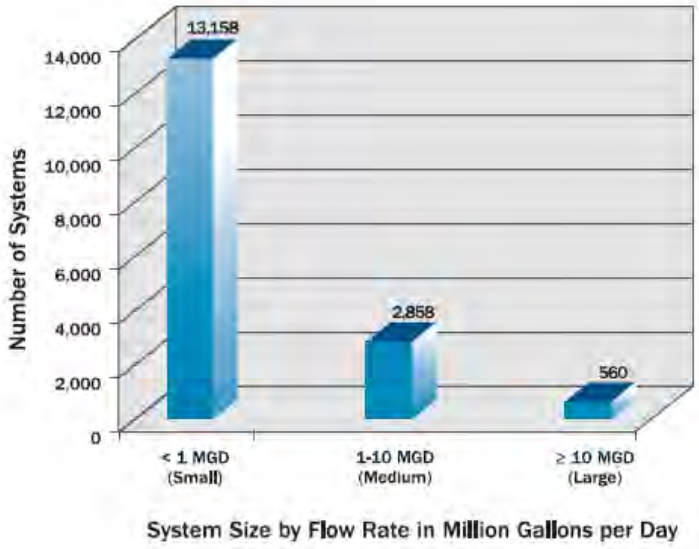
Wastewater

- Disruption of a wastewater treatment utility or service can cause loss of life, economic impacts, and severe public health and environmental impacts.
- If wastewater infrastructure were to be damaged, the lack of redundancy in the Sector might cause denial of service to domestic and industrial users.
- The majority of utilities are small in size, and provide wastewater treatment to approximately 23 million people (Figure 2).
- The medium or large size utilities systems serve the majority, at about 90 percent of the population.

Water Sector Overview

- **Comprises approximately 155,000 public drinking water systems (includes both community and non-community water systems, such as schools, factories and campgrounds) and approximately 16,500 publicly owned wastewater treatment utilities (EPA, 2012 and DHS, 2010).**
- **Water utilities consist of source waters, treatment facilities, pumping stations, storage sites, and extensive distribution, collection, and monitoring systems.**
- **The Water Sector is vulnerable to a variety of all-hazard threats including contamination with deadly agents; insider threats; physical attacks using improvised explosive devices (IEDs); cyberattacks; and natural hazards.**
- **Successful attacks on a drinking water or wastewater system could result in large numbers of illness, casualties, and denial of service, which could severely impact the Nation's public health and economic vitality.**

Figure 2: Publicly Owned Wastewater Treatment Works and System Size



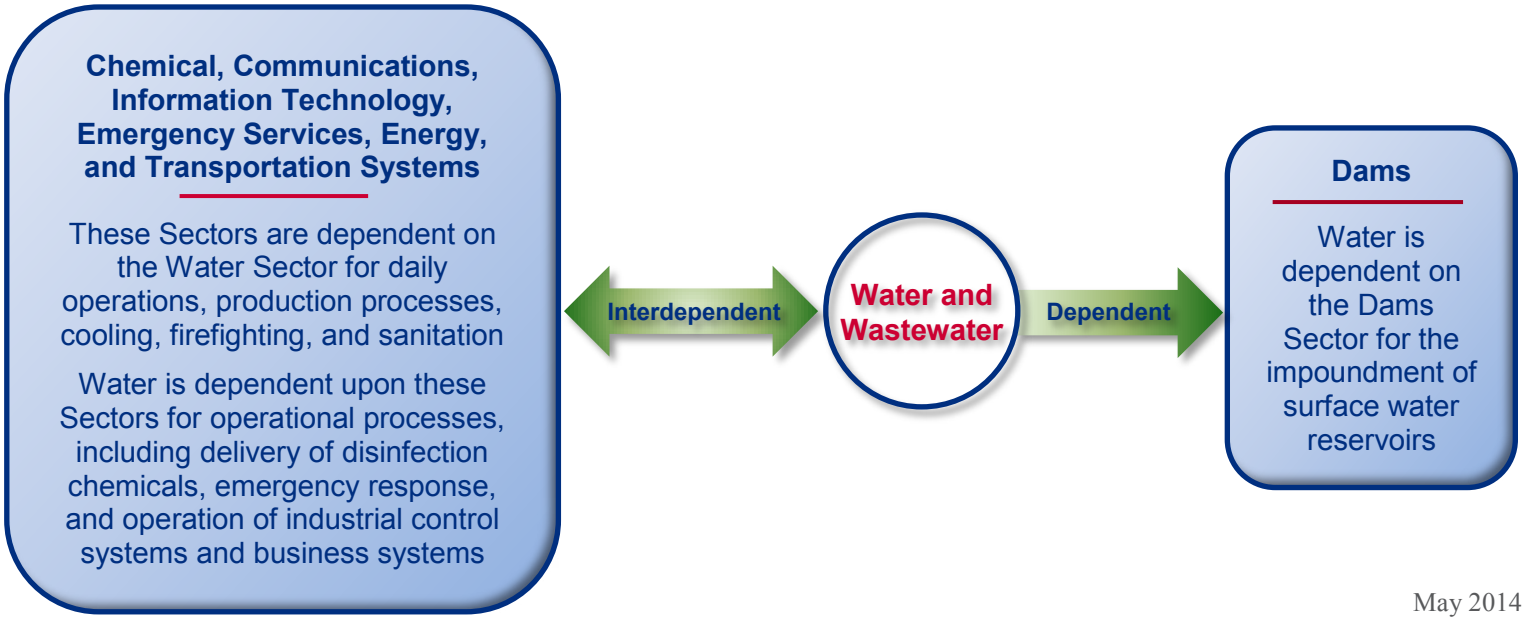
Threats and Hazards of Significant Concern

- **Chemical, Biological, or Radiological Contamination**
  - Most public water supplies are monitored and treated to prevent the distribution of contaminated drinking water.
  - The risk of CBR contamination stems from both the enduring terrorist threat to contaminate the U.S. water supply and the serious health impacts that could result from an undetected contaminant.
  - These impacts could vary depending on the type of substance, route of exposure (ingestion, absorption, inhalation), and amount of time before the contaminant is detected.
- **Natural Hazards**
  - Natural hazards, such as hurricanes, tornadoes, floods, earthquakes, and drought, pose a serious and continuing risk for the Sector.
  - Water infrastructure may be severely disrupted or destroyed by such hazards, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies (Figure 3).
  - Critical water shortages may also result from drought conditions and climate change, leading to water use restrictions and rationing.
- **Physical and Cyberattacks by Terrorists, Homegrown Extremists, or Disgruntled Insiders**
  - Physical attacks using IEDs on chemical storage tanks or other critical nodes in a drinking water or wastewater system could result in a release of hazardous materials or in a long-term loss of service should a "single-point-of-failure" be destroyed.
  - Cyberattacks and intrusions on supervisory control and data acquisition (SCADA) systems or other business systems pose a serious threat to the Water Sector, allowing malicious actors to manipulate or exploit control systems essential to operation of drinking water and wastewater utilities.

For More Information

- Sector-Specific Agency: Environmental Protection Agency, www.epa.gov/
- Environmental Protection Agency (EPA), Water Security, http://water.epa.gov/infrastructure/
- DHS, *Infrastructure Protection Report Series: Community Water Systems (CVPIPM)*, version: 29 August 2011
- DHS and EPA, *2010 Water Sector-Specific Plan*, hwww.dhs.gov/files/programs/gc_1179866197607.shtm
- DHS, *National Risk Profile,* OCIA@hq.dhs.gov

Figure 3: Common, First-order Dependencies and Interdependencies of the Water Sector



May 2014

Homeland Security

Prepared by the DHS National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Questions or comments should be directed to OCIA@hq.dhs.gov

The Office of Cyber and Infrastructure Analysis (OCIA) produces Sector Risk Snapshots in support of the Homeland Security Enterprise as part of the Department's efforts to carry out comprehensive assessments of the risks to critical infrastructure, and to facilitate a greater understanding of the emerging threats to and vulnerabilities of critical infrastructure in the United States. For more information, contact OCIA@hq.dhs.gov or visit our Website at www.dhs.gov/office-cyber-infrastructure-analysis.

Homeland Security

IECC Cyber Vulnerabilities Whitepaper

Communications Sector

January 2018

LTC David L. Skalon
2 January 2018

BACKGROUND:

Reliance upon an interconnected backbone as an enabler to other sectors has evolved from convenience to necessity. "Over the last 25 years, the (telecommunications) sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems."[1] With this reliance comes the burden of securing transmissions while meeting the growing need for bandwidth. When considering the playing field for this sector, like many other Indiana sectors, it is a divide between the larger corporations and the smaller, mom and pop providers.

The appetite for connectivity has grown exponentially and reaches down to children of a decreasing age every year. Today's generation does not know of a time without the internet and demands its availability and reliability. Providing that backbone has necessitated the moves to the various platforms and systems listed previously. This reliance makes it a desirable target for emotional and financial impact, but where does the risk really exist?

GOVERNANCE, REGULATORY AND SUPPORT ASSOCIATIONS:

- U.S. Department of Homeland Security (DHS) - Designated as the lead agency for the Communications Sector at the national level.
- Indiana Utility Regulatory Commission (IURC)- Monitors and evaluates regulatory proceedings and policy initiatives at the federal, state, and local levels that affect telephone, cable, and internet service providers in the state.
- Federal Communications Commission (FCC)- Regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories.
- Indiana Exchange Carrier Association (INECA)- Advocates for its member companies on federal and state issues, to educate government leaders as well as the public at large on the importance of modern telecommunications to rural communities.
- Indiana Broadband Telecommunications Association (IBTA)- Trade association representing Indiana's Broadband and Technology industry.
- National Exchange Carrier Association (NECA)- Supports local telecommunications companies. We are dedicated to helping our members provide broadband-based solutions to keep their customers connected.
- National Rural Telecommunications Cooperative Association (NRTC)- Provides solutions that help our electric and telephone members bring all of the advantages of today's evolving technology to rural America.

[1] DHS, https://www.dhs.gov/communications-sector, details the national perspective of this sector, retrieved February, 2018.

- National Telecommunications and Information Administration (NTIA)- Executive Branch agency that is principally responsible for advising the President on telecommunications and information policy issues.
- National Telecommunications Cooperative (NTCA)- The Rural Broadband Association is the premier association representing nearly 850 independent, community-based telecommunications companies that are leading innovation in rural and small-town America.
- North American Numbering Plan Administration (NANPA)
- United States Telecom Association (USTA)

RISKS:

The infrastructure is vast and diverse, many different types of risks could compound to make widespread outages possible. The risks span from basic outages to 2nd and 3rd order effects that could put many people in harm's way as depicted below:

1. Natural disasters and extreme weather have increased in frequency and severity over the past few years with varying levels of impact to our communication infrastructure. In Indiana, the most likely threats are floods, snow storms, and tornados. Solar flares from the sun also pose a less frequent, but potential threat as well.
2. The Communications Sector depends on suppliers for the products and services that are necessary to deliver communication services to users. In particular, the sector is dependent on reliable hardware and software. This is an area the sector continues to scrutinize closely.
3. Cyber threats include the typical software and hardware exploits that impede the end user's devices, but these attacks can have a cascading impact on the infrastructure it operates on.
4. Larger providers have the staff and processes to prevent and mitigate known risks and train their personnel on best practices. Smaller providers do not have the capital or expertise to prevent or react at the same level as the larger providers.

PAST ATTACKS:

Although the media is now starting to cover cyber attacks at an increased rate, it is still not real to the average consumer, unless they have experienced and outage or inconvenience. Attacks like the one in a region of California from 2015 details the impact that physical attacks have on infrastructure:

Someone continues to target critical communications infrastructure in a region of the U.S., on Monday, September 14, unknown attackers cut backbone fiber optic Internet cables in Livermore California. This is not an isolated attack, law enforcement counted fourteenth attacks on critical communications infrastructure in the same region and security experts suspect that the attackers are carrying out the sabotage for economic and cyber warfare.

The investigation on such kind of attacks is conducted by the FBI because AT&T's fiber optic network is considered to be part of the nation's critical communication infrastructure.

"Someone deliberately severed two AT&T fiber optic cables in the Livermore, Calif., Monday night, the latest in a string of attacks against the Internet's privately run backbone.*" reported the USA Today website.*

SECTOR SPECIFICS:

The communications sector has several subsections to it: telephone companies, wireless providers, Internet and Voice over Internet Protocol (VOIP) providers, and Cable/Internet providers. Indiana has been known to have a lot of small or 'mom and pop' utilities and the telecommunications sector is no different. However, based on scope and impact to the national infrastructure, some nodes within the state have a higher risk associated with them. Some of these are run as cooperatives or by local municipal/city councils, etc; it varies by location.

BOTTOM LINE:

In light of the challenges stated above; aging infrastructure, competition between repairing infrastructure vs improving cyber security and the clear lack of governance as it relates to cyber security leave this sector somewhat vulnerable to attack as compared to other critical infrastructure sectors. The level of risk is based on scale. Larger providers have robust architecture, security processes and protocols to minimize impact. Smaller providers is where the higher risk is found. The recommended approach to these elements is outreach and education to initiate the actions to protect. The awareness factor alone can prevent the lower echelon threats while improving the overall health of our telecommunication services.

IECC Cyber Vulnerabilities Whitepaper

Energy Sector

February 2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Cyber Vulnerabilities Whitepaper - Energy Sector

Carl A Cahill
Walter Grudzinsk
Stan Partlow Jr.
27 February 2018

BACKGROUND:

The Energy Sector powers the lives and businesses of Indiana residents. Computers, traffic lights, water pumps, furnaces, air conditioners, ATMs, stoves, refrigerators, and many other devices require electricity. Innovation continues to drive new uses for electricity by integrating computers with day-to-day devices as the Internet of Things (IoT) rapidly expands.

Power is the foundational component of modern society. Presidential Policy Directive 21 states the Energy Sector is "uniquely critical" as it enables all other critical sectors.[1] The Energy Sector is classified as Critical Infrastructure and is heavily regulated to ensure the reliability of power to residents and businesses.

Cybersecurity is a key topic in the Energy Sector due to the potential impacts disruption of power could have to society. Cyber threat actors have shown an increased interest in having capabilities to disrupt the generation and distribution of power.[2] The Energy Sector remains focused on providing reliable power through resilient and defensible systems.

GOVERNANCE, REGULATORY AND SUPPORT AGENCIES:

- Federal Energy Regulatory Commission (FERC) – is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. FERC has additional powers and responsibilities outlined in The Energy Policy Act of 2005.[3] https://www.ferc.gov/
- Indiana Utility Regulatory Commission (IURC) – Energy Division Regulates pricing models and quality of service but stops short of mandating cyber defense standards. https://www.in.gov/iurc/2340.htm
- North American Electric Reliability Corporation (NERC) – is an international not-for-profit regulatory authority responsible for assuring reliability and security of the bulk power system in North America. NERC is responsible for publishing Critical Infrastructure Protection (CIP) physical and cybersecurity requirements to protect bulk electric systems. http://www.nerc.com/Pages/default.aspx
- ReliabilityFirst Corporation (RFC) – is the regional organization, approved by FERC, responsible for the reliability of the North American Bulk-Power system in Indiana. https://www.rfirst.org/
- Department of Energy (DOE) – federal agency tasked with advancing the Energy Sector and enabling reliable and resilient energy at the federal level. https://energy.gov/
- Federal Bureau of Investigations – is the government agency responsible for investigating cyber-crime. https://www.fbi.gov/
- Department of Homeland Security (DHS) – is the government agency responsible for assisting critical infrastructure with combating cyber-crime. https://www.dhs.gov/

---

[1] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[2] https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=5F40E0A2-B836-40EA-ACC6-9BF3B43A1B8F
[3] https://www.ferc.gov/about/ferc-does.asp

RISKS:

Impacts of a successful cyber-attack on a utility company vary greatly depending on the motivation of the threat actor, the depth of the infiltration, and the sophistication of the utility's defenses. The two highest risk scenarios are:

1) The disruption of the generation and distribution of power.
2) The loss of Customer personally identifiable information (PII)

Impacts and likelihood of a cyber event resulting in the disruption of the generation and distribution of power continue to be a point of debate within the Nation. The threat actors capable of performing this type of attack consist primarily of Nation States. Nations States are unlikely to attack the grid due to the threat of military action. The impacts of such an event will depend on the duration of power disruption and the scale of population affected. Loss of power for a few hours will result in some economic loss. Longer term, large scale power loss can lead to society breakdowns as basic necessities such as food, water, and livable shelter become scarce. 2016 marked the development and use of the first ever malware framework built specifically to attack the power grid.[4] Malware such as Crashoverdrive demonstrate threat actors are motivated to have capabilities to disrupt power.

Theft of Customer PII is likely performed by a different threat actor than those looking to attack the power grid. Cyber criminals are motivated to steal PII for financial gain. Energy companies keep social security numbers for Customers and in some cases credit card and bank account information. All three data types are highly desirable for financially motived threat actors. Energy Companies have different methods for preventing the loss of Customer PII including the use of encryption, least privilege, and network segmentation.

PAST ATTACKS:

A significant increase in Industrial Control System (ICS) based cyber activity highlighted 2016 and 2017 for the Energy Industry. Five unique ICS threat actors were active and two ICS specific malware variants were discovered.[5] Also disruptive IT malware, such as WannaCry, became a potential concern for the Energy Industry.

The Energy Industry has experienced a small number of successful targeted attacks over the last 10 years. Most of the threat actors targeting the disruption of the power grid are Nation States. Nation States are less likely to execute an attack and more likely to stage malware for future attacks if needed in a time of war or to make a political statement.[6]

Stuxnet – In June of 2010 the first cyber-attack on the Energy Industry took place on an Iranian nuclear power plant. The United States and Israeli governments are suspected to have developed and executed this cyber-attack.

Ukraine – in 2015 and 2016 the Ukraine experienced power outages due to cyber-attacks. A framework specific to the Energy Industry was used in the 2016 cyber-attack. The threat actor Electrum, with ties to

---

[4] https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
[5] https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=5F40E0A2-B836-40EA-ACC6-9BF3B43A1B8F
[6] https://www.csoonline.com/article/3260624/critical-infrastructure/insecure-by-design-what-you-need-to-know-about-defending-critical-infrastructure.html

Sandworm, was responsible for the 2016 Ukraine attack. The CRASHOVERRIDE, an ICS specific malware framework, was developed and used in this attack.

Nuclear 17 / Palmetto Fusion – In 2017 Energy companies in the United States were targeted by threat actors. A nuclear power plant in Kansas had non-Nuclear controls systems compromised.[7] This cyber-attack started with a phishing campaign. Russia-based threat actors are suspected in this targeted attack.

UK / Ireland – Russia-based threat actors target the UK and Irish power grid in a series of cyber-attacks in 2017. Power was not disrupted. Investigators suspect Russia was attempting to put malware on systems to use at a later date to potentially disrupt the grid and cause power outages.[8]

SECTOR SPECIFICS:

The Energy Sector is regulated and partners closely with government agencies. Relationships with both regulators and government agencies has helped advanced and formalize some cyber capabilities for the industry.

FERC and NERC provide oversight for cybersecurity controls to support reliability requirements for the Bulk-Electric Systems. NERC has issued prescriptive controls known as Critical Infrastructure Protection (CIP) which are audited and enforced.

The Department of Homeland Security (DHS), Department of Energy (DOE), and Federal Bureau of Investigations (FBI) continue to develop programs such as Enhanced Cybersecurity Services (ECS), Cybersecurity Risk Information Sharing (CRISP), and Electricity Sector Information Sharing and Analysis Center (E-ISAC). These programs help participating utilities detected and protect against advanced cyber threats through analysis and information sharing.

The Energy Sector has a unique program called Cyber Mutual Assistance (CMA). CMA is an agreement between participating utilities to provide support during a cyber event. Support might include sending cybersecurity experts to a utility in need to help defend the network or send IT personnel to assist with recovering systems. This program is similar to the way utilities share resources to help restore services after a large storm, but for cyber events.

BOTTOM LINE:

Loss of power to a region has negative economic impacts and may lead to safety issues for the population. Electricity is needed for society's basic needs - water, food, heating/air, medical care, and transportation.

Within the State of Indiana cyber-defense capabilities vary greatly depending on the size of the utility. Smaller utilities are less likely to have dedicated cybersecurity staff and budgets than large utilities. Cyber regulations such as NERC CIP help protect the power grid from commercial malware and normal cyber threat actors.

Additional cybersecurity capabilities are needed to identify, protect, detect, and respond against advance threat actors. As stated in this document, Nation State actors, have targeted the United States power grid. This trend is unlikely to change in the near future. Both government and private industry need to continue working together to make the power grid both resilient and defensible.

---

[7] https://www.wired.com/story/hack-brief-us-nuclear-power-breach/

[8] https://www.thesun.co.uk/news/4915334/russian-hack-attack-on-britain-energy-grid-cyber-crime/

IECC Cyber Vulnerabilities Whitepaper

Water and Wastewater Sector

February 2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Cyber Vulnerabilities Whitepaper - Water and Wastewater Sector

David B. Tygart
12 February 2018

BACKGROUND:

Many water and wastewater utilities within the State of Indiana, particularly small systems, lack the resources for information technology (IT) and security specialists to assist them with starting and maintaining a cybersecurity program. "Utility personnel may believe that cyber-attacks do not present a risk to their systems or feel that they lack the technical capability to improve their cybersecurity."[1]

The basic problem for water utilities today is the convergence of two systems that used to be relatively segregated: information technology (IT) and operational technology (OT). IT is what a layperson commonly associates with cyber threats: the computer systems that are linked to the internet for email, billing, bookkeeping, and desk work. Viruses enter these systems through a mess of pathways: infected USB drives, email attachments, bad links on compromised websites or even the late night operator linking his iPhone TV to a control computer.[2]

The National Infrastructure Advisory Council, a group of experts that advises the Department of Homeland Security and the president on critical infrastructure, says that cybersecurity awareness among water utilities is "often limited" and that the number of cybersecurity experts in the sector is "insufficient for current needs.[3]

According to the U.S. EPA, Indiana's water and wastewater infrastructure needs a total of nearly $14 billion over the next 20 years to update an aging infrastructure.[4] These costs will compete against the need to improve Cyber Security within this sector.

GOVERNANCE, REGULATORY AND SUPPORT AGENCIES:

Wastewater companies require an annual re-certification of their license to operate, but water companies do not. They use the one they get when they start to operate. New State of Indiana legislation was introduced during the FY18 session. Bill number: SB 362 subject: "Regulation of Water and Wastewater Systems." The bill establishes new requirements for water treatment plants and wastewater treatment plants applying to the Department of Environmental Management for the issuance or amendment of a permit, including a cost-benefit analysis, a capital asset management plan, and a cybersecurity program. Unfortunately, this bill as written might not hit the mark on getting water companies to comply. In addition, as there is no clear standard as to what a "cyber plan" is, not sure if we would get any statewide useful information.

- U.S. Environmental Protection Agency (EPA) - is the designated as the lead agency for the Water and Wastewater Sector.
- Indiana Utility Regulatory Commission (IURC)- Water/Wastewater Division Regulates pricing models and quality of service but stops short of mandating Cyber Defense standards.
https://www.in.gov/iurc/2338.htm

---

[1] Implementing A Cybersecurity Program At Your Water Or Wastewater Utility; Office of Water (MC 4608-T) EPA, August 2016; https://www.asdwa.org/wp-content/uploads/2016/07/Cybersecurity-Guide-for-States_Final.pdf
[2] http://www.circleofblue.org/2016/world/water-sector-prepares-cyberattacks/
[3] https://www.dhs.gov/sites/default/files/publications/niac-water-resilience-study-slidedeck-qbm-03-14-16-508.pdf
[4] Indiana Utility Regulatory Commission 2016 Annual Report http://www.in.gov/iurc/files/Annual%20Report%202016%20WEB%20version.pdf

- Water and Wastewater Sector Coordinating Council (SCC) - An EPA organized council bringing Federal, State, and local entities, and owners and operators of water utilities together and are responsible for planning and implementing the Sector's security and resilience activities. https://www.waterisac.org/
- Water Information Sharing and Analysis Center, is the designated communications and operations arm of the United States water and wastewater sector. With an all - hazards focus

RISKS:

In the drinking water and wastewater sub-sectors, a cyber-attack could cause chemical contamination, biological contamination and/or physical disruption through the manipulation of specialized computer systems controlling essential infrastructure known as Supervisory Control and Data Acquisition (SCADA) systems. A successful attack could cause major damage, resulting in long periods of operational downtime, financial losses, loss of public trust and most importantly, a threat to public safety.

Unlike the loss of power to the public sector, due to a cyber-attack, the contamination to a public water source thought the manipulation of industrial control systems may go undetected for hours to days having adverse effects on the general population.

PAST ATTACKS:

According to a news report from International Business Times, hackers were able to change the levels of chemicals used to treat tap water during an attack on the outdated IT network of one U.S. plant by exploiting its web-accessible payments system and using it to access the company's control systems.[5]

For eleven days in 2013 an Iranian computer hacker gained access into the computer system that controls Bowman Dam, in Rye, New York. City officials were unaware that they were being hacked until contacted by the Department of Homeland Security. The Iranian computer hacker tapping into the supervisory control and data acquisition system was able to learn water levels and temperatures as well as the status of the sluice gate, which controls the flow of water. Fortunately, the attacker was unable to operate the gate from Iran because that particular control system had been disconnected for maintenance.[6]

SECTOR SPECIFICS:

Most of the water systems in the state are owned by municipal or not-for-profit entities. These entities are managed by a board of directors or town or city councils. According to the 2013 "Water Utility Resource Report: A Look at Indiana's Water Supply & Resource Needs" report prepared by the Indiana Utility Regulatory Commission 487 of 555 utilities surveyed submitted data for evaluation. From the data, 69% are municipal utilities. Not-for-profit and investor owned utilities made up 17% and 11% of respondents, respectively. Conservancy districts, cooperatives, and regional water districts are less common and combined made up less than 4% of respondents.[7] Many industrial businesses self-produce their water and wastewater requirements.

Automation controllers or PLC's within this sector have a long life cycle before replacement 10-20 years. As many of these were designed and install prior to all the cyber concerns many are lacking fundamental blab la

[5] https://www.infosecurity-magazine.com/news/water-treatment-plant-hit-by/
[6] http://www.circleofblue.org/2016/world/water-sector-prepares-cyberattacks/
[7] https://www.in.gov/iurc/files/Water_Utility_Resource_Report-_FINAL-_8282013_with_cover(1).pdf

BOTTOM LINE:

In light of the challenges stated above; aging infrastructure, competition between repairing infrastructure vs improving cyber security and the clear lack of governance as it relates to cyber security leave this sector extremely vulnerable to attack as compared to other critical infrastructure sectors. The results, unlike most other sectors, could have immediate and catastrophic impact on a population. Our approach must be thru outreach and education if we are to see improvements.

IECC Pre- through Post-Incident White Paper

Education Sector

2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Pre- through Post-Incident White Paper — Education Sector

David Greer, Project Lead the Way
Andrew Korty, Indiana University
William Mackey, Indiana State University
Darryl Togashi, Ivy Tech Community College

BACKGROUND:

The education sector in the State of Indiana consists of a wide range of institutions: K-12 schools, two- and four-year colleges, vocational colleges, and large research universities. While each of these institutions faces similar cyber risks, the resources they have available for a complete cybersecurity program to prepare for, respond to, and recover from cyberattacks are quite variable. Specific gaps, as in most industries, include employee training, robust data backups, and a strong cybersecurity operations function.

Unlike other industries, the education sector has traditionally given broad leeway to faculty, staff, and students to choose their own technology and use it in almost any way they feel appropriate. This culture, present more in higher education than in K-12s, is meant to contribute to academic freedom and the ability to teach, learn, and do research unfettered by excessive policies and technical limitations. While this culture may seem at odds with cybersecurity best practices, the two can coexist peacefully if the business needs and the threat profile of the institution are carefully weighed and considered.

Although the risks in the education sector don't usually result in immediate threats to public safety as they can with some utilities, there are some physical security considerations, especially given the large physical plant of some institutions. The vast computing and communications capabilities of large universities can also be of interest to attackers. But an educational institution's most commonly targeted resource is its stores of personal and institutional data.

GOVERNANCE, REGULATORY AND SUPPORT AGENCIES:

LEVEL	AGENCY/BODY	DESCRIPTION
Federal	U.S. Department of Education	The U.S. Department of Education (US DOE) is responsible for implementing federal laws related to the education system, including students. The agency's primary responsibility is the Elementary and Secondary Education Act (ESEA) of 1965 as amended by the Every Student Succeeds Act (ESSA) of 2015. US DOE is also responsible for various other laws, including[1]: - Family Educational Rights and Privacy Act - Individuals with Disabilities Act - Civil Rights laws, including the Title II of the Americans with Disabilities Act, Title IX of the Education Amendments of 1972, and Title VI of the Civil Rights Act - Workforce Innovation and Opportunities Act

[1] https://www2.ed.gov/policy/landing.jhtml?src=pn

		- Carl D. Perkins Career and Technical Education Act of 2006[2]
Federal	Federal Trade Commission	The Federal Trade Commission (FTC) manages the Children's Online Privacy Protection Act (COPPA) which is a law created to protect the privacy of children under 13. The Act specifies: - That sites must require parental consent for the collection or use of any personal information of young Web site users. - What must be included in a privacy policy, including the requirement that the policy itself be posted anywhere data is collected. - When and how to seek verifiable consent from a parent or guardian. - What responsibilities the operator of a Web site legally holds with regards to children's privacy and safety online, including restrictions on the types and methods of marketing targeting those under 13.
Federal	Federal Communications Commission	As it relates to education, the FCC's ole is related to the governance of the E-Rate program. E-Rate is administered through the Universal Service Administrative Company[3].
Federal	Department of Health and Human Services – Office of Civil Rights	The Department of Health and Human Services' (HHS) Office for Civil Rights is responsible for enforcing the Privacy and Security Rules.
Federal	U.S. Department of Housing and Urban Development	HUD administers the ConnectHome initiative, which is focused on "increasing access to high-speed internet for low-income households". ConnectHome partners with local libraries, schools, private providers, and HUD housing units to fulfil its mission[4].
Federal	U.S. Department of Education, Office of Education Technology	Issues related to technology, infrastructure, and cybersecurity can be found across the many laws and initiatives implemented by US DOE and other federal agencies. However, US DOE has attempted to centralize these issues in its Office of Educational Technology[5]. Guidance and resources on how these laws affect technology issues for both State Education Agencies and Local Education Agencies can be accessed through this office.
State	Indiana General Assembly	Article eight of the Indiana Constitution as amended 2016 states: Knowledge and learning, generally diffused throughout a community, being essential to the preservation of a free government; it shall be the duty of the General Assembly to encourage, by all suitable means, moral, intellectual, scientific, and agricultural improvement; and to provide, by law, for a

[2] https://www2.ed.gov/policy/sectech/leg/perkins/index.html
[3] http://www.usac.org/sl/
[4] https://connecthome.hud.gov/
[5] https://tech.ed.gov/

		general and uniform system of Common Schools, wherein tuition shall be without charge, and equally open to all[6]. The General Assembly therefore establishes laws that: - Grant administrative powers to the State Board of Education; - Prescribe the method of selection, tenure, duties, and compensation of the State Superintendent of Public Instruction; - Manage the Common School fund; - Grant specific authorities to Local Education Agencies, known as School Corporations; and - Establish broad education policies.
State	Indiana State Board of Education	The Indiana State Board of Education (SBOE) is established in Indiana Code Title 20, Article 19, Chapter 2[7]. The SBOE is granted with a host of powers and responsibilities, including the ability and responsibility to adopt administrative rules under IC 4-22-2[8] concerning education policies and procedures as outlined in IC 20-19-2-8[9]. Generally speaking, the duties of SBOE are to: - Establish the educational goals of the state, developing standards and objectives for local school corporations; - Assess the attainment of the established goals; - Assure compliance with established standards and objectives; - Coordinate with the commission for higher education and the department of workforce development to develop entrepreneurship education programs for elementary and secondary education, higher education, and individuals in the work force. - Make recommendations to the governor and general assembly concerning the educational needs of the state, including financial needs; - Provide for reviews to ensure the validity and reliability of the statewide assessment program; and - Oversee the distribution of certain federal aid programs.
State	Indiana Department of Education	Indiana Code 20-19-3 establishes the Department of Education. The State Superintendent of Public Instruction, as established and governed by Indiana Code 20-19-1-1 (IC 20-19-1-1.1 beginning January 10, 2025), is the director of the department. The specific duties and responsibilities of the department are established in both Indiana Code set by the General Assembly and administrative rules adopted by the State Board of Education. Generally speaking, it is the department's responsibility to implement the education laws, policies, and procedures set by

[6] https://iga.in.gov/legislative/laws/const/

[7] http://iga.in.gov/legislative/laws/2017/ic/titles/020#20-19

[8] http://iga.in.gov/legislative/laws/2017/ic/titles/020#4-22-2

[9] http://iga.in.gov/legislative/laws/2017/ic/titles/020/#20-19

		state law and administrative rules. Many of these responsibilities relate to monitoring and supporting local school corporations.
Local	School Corporations	Indiana Code 20-26 defines local school corporations and their powers and duties. The extent to which Indiana favors local control of schools is well represented by IC 20-26-3 – Home Rule, which states: - "Notwithstanding any other law and subject…the policy of the state is to grant to each school corporation all the powers needed for the effective operation of the school corporation."[10] - "The rule of law that any doubt as to the existence of a power of a school corporation must be resolved in favor of the existence of the power."[11] By law, school corporations: 1. **Must** adopt discipline rules that prohibit bullying, which includes bullying that may occur through the use of data or computer software (IC 20-33-8-13.5) and provide training to its employees and volunteers concerning the school's bullying prevention and reporting policy (IC 20-26-5-34.2). 2. **May** offer classes, instruction, or programs regarding the potential risks and consequences of creating and sharing sexually suggestive or explicit materials through cellular telephones, social networking web sites, computer networks, and other digital media.

RISKS:

Educational institutions have large repositories of personal and institutional data, much of which is regulated (see above). Institutions must safeguard this data and the systems that process it while staying true to mission of teaching, research, and community partnership. Many of the safeguards, which include employee training to prevent successful phishing attacks, regularly tested data backup systems to allow recovery from ransomware attacks, highly trained security operations and incident response teams, and others, can be beyond an institution's budget capacity, especially for smaller institutions.

Schools, especially universities, are more akin to cities than companies, with up to 100,000 people using technology independently. As mobile devices and cloud services proliferate, education sector users are becoming ever more independent, and the institution is losing the ability to implement safeguards that can reach all devices and services. Keeping devices secure therefore falls increasingly to the end user, yet due to the sheer number of people involved, training costs escalate quickly. Further, relatively little standardization of training or safeguards exists across the sector, making it difficult to achieve efficiencies through collaboration.

---

[10] IC 20-26-3-1

[11] IC 20-26-3-2

Few institutions have the budget for a cybersecurity operations center (CSOC), yet given the way technology has changed and threats have evolved, a CSOC is quickly becoming an essential pillar of any cybersecurity program. Gartner writes

> The traditional thinking is that, although the organization does not control the threats, it can control vulnerabilities, and thus, there is a need to focus there. At many organizations, increasing IT complexity and the emergence of bring your own device (BYOD) break down any semblance of control over assets and their vulnerabilities, making vulnerability-centric security much harder, if not impossible. Threat intelligence is a critical tool for enabling the threat-centric side of a security equation and, at least in part, taking the fight to the adversary by identifying, exposing and sometimes prosecuting the threat actors.[12]

The takeaway is that any mature cybersecurity program needs to include cybersecurity operations with a strong threat intelligence component.

But cyberspace isn't the only arena in which cybersecurity funding has an impact. Many colleges and universities have the added responsibility of protecting students that live on campus. While public safety is not a direct concern of cyber risk, many cyber resources are used for life and safety protection. An attacker could target door access control or video surveillance systems to gain access to student living areas and cause harm. Also of concern are blended attacks, in which attackers disable alarm or emergency communication systems just before launching a kinetic attack, thereby increasing damage by reducing the ability of public safety personnel to react and respond.

SECTOR SPECIFICS:

Public and private institutions alike aim to foster an environment of academic freedom, and a traditional, by-the-book approach to cybersecurity is often met with resistance. Particularly in colleges and universities but also in some K-12 environments, CISOs and security practitioners must take a risk-based approach with strict attention to every safeguard's impact on academic and business function. Also, the education CISO's ability to implement safeguards is often constrained by very limited budgets for cybersecurity. These two factors create a unique and challenging cybersecurity environment.

Colleges and universities have shown particular leadership in all types of information sharing, including cybersecurity information. The Research and Education Network Information Sharing Analysis Center (REN-ISAC) consists of 540 member institutions around the world, eight of which are Indiana-based, and is one of higher education's most vibrant information sharing communities. Security practitioners at member schools share threat intelligence, awareness materials, and best practices on a daily basis, and this network of individuals can prove invaluable when coordinating incident response among multiple institutions.

Because of this established culture of information sharing, it's likely that any institution experiencing an incident or attack will request and receive assistance from trusted peers before turning to other groups. It would be rare for educational institutions to accept help from volunteer or National Guard forces in these situations.

PAST ATTACKS:

The 2014 Symantec Internet Security Threat Report puts the educational sector 3rd in number of cyberthreat incidents per year (behind only healthcare and retail)[13]. Since Indiana Code article 24-4.9 requires businesses and other organizations to notify affected consumers following the discovery of a

---

[12] Gartner, *How to Collect, Refine, Utilize and Create Threat Intelligence*, 2016

[13] Symantec Internet Security Threat Report, 2014

personal data exposure as well as the Attorney General's office, we can assume that publicly available data on exposures affecting Indiana educational institutions is reliable.

Indiana educational institutions have reported 29 reported data breach incidents since 2005. That translates into around 3 reported breaches of personal information from Indiana educational institutions each year, for the past 17 years[14]. The data show that, by year, there is not a statistically significant change in the number of breaches. Moving beyond just Indiana, however, 872 breaches have occurred in the education sector alone across the United States, giving us an average of 2.4 breaches per day[15].

Institutions seem to be particularly vulnerable to social engineering campaigns, as a major goal of every university is to foster a sense of 'welcome'. This often times includes allowing students, parents, and friends to bring and connect to their own personal devices. Moreover, student records can become a wealth of lucrative information for potential offenders.

BOTTOM LINE:

As in other sectors, many educational institutions lack the resources to develop and maintain a complete cybersecurity program. Schools that are deficient are particularly vulnerable to threats such as social engineering, ransomware, system intrusions, and denial of service attacks. One of the most commonly reported gaps is in training, in the areas of system maintenance and security (for IT staff), social engineering avoidance, and best practices for data protection. Also typically lacking is a solid security operations program using threat intelligence. As institutions put more resources into cybersecurity, these two areas are likely to receive the most focus.

---

[14] Mackey, *Summary of Questionnaire for Education Sector for the Current State of Cybersecurity in Indiana*, 2018

[15] Center for Digital Education

Indiana National Guard (INNG)

State Cyber Baseline Survey Results

2018

Purpose

This survey was designed to better understand what other states are doing to support these local governments in the support for critical infrastructure cyber protection. The survey was sent through J3 channels to all states and 8 states responded.

Survey Questions:

Many states use their National Guard cyber forces to assist in protecting the networks in their state. According to a National Governors Association (NGA) memo, there were 32 cyber response plans among the 26 states surveyed. In particular California, Michigan, Ohio, and Washington have been working in this area for a number of years. In almost all instances the duty is performed in a state active duty (SAD) status and the soldiers are paid from state funds. Although, Ohio does do some work in non-SAD capacity it is in Inactive Duty Training (IDT) status and the event is geared toward training for their team. The work performed ranges from penetration testing and network vulnerability assessments to assisting local governments, as in Michigan, during the Flint water crisis.

To help develop this document INNG J36 has teamed up with the office of Homeland Security & Public Safety Division NGA Center for Best Practices National Governors Association.

?Q-1. We are interested in finding out if you are conducting vulnerability assessment and/or penetration (PEN) testing with non-DODIN entities within your state? Specifically:

- With whom i.e. State agencies, private companies (critical infrastructure owners) and local governments?
- How are you funding the assessments/PEN testing (SAD, IRT) and who is doing it (DCO-E, CPT, other)?
- How often have you executed those assessments over the past year and the plan sustainable?
- What type of testing, PEN or vulnerability Assessments?
- Do you have TTPs/processes or other information you can share for these engagements.

In Indiana we don't see PEN testing or vulnerability assessments as a "fix all" for the state. We see it more as a way to bring credibility to the need for better awareness and training. We also see it as a way to support the justification to exercise cyber defense within the State's critical infrastructure sectors beyond the energy sector. Our focus currently is with water delivery and election sectors. We are developing plans to exercise these sectors in the next 18-24 months. We will continue participating in the annual GRIDEX Energy sector exercise.

?Q-2. Does your state have a Cyber Response Plan that identifies use of your National Guard assets to assist? Specifically:

- Are you/have you worked with your State on a Cyber Response Plan?

- Is your organization part of the decision making process during a Significant Cyber Incident?
- Have you or are you planning to exercises C2 with the state emergency management teams?

The State Government of Indiana is working to revise its Cyber Response Plan and currently completing the research phase. For the Indiana National Guard we own the "Pre and Post" cyber incident portion of the plan. In the "Pre" phase we are faced with an estimated 8000 entities that could use Cyber assessments. Even if we were to team up with DHS and other private capabilities it is a bridge to far. Not to mention the limitations placed on the DoD under the Economy Act. We see the best use of our limited assets to support outreach as stated above and focus any PEN testing towards State Government agencies. In a "Post" cyber incident scenario we would be in a supporting role to the DHS or other State agencies. Our plan is to develop whole of state government exercises in the future to develop these relationships and processes.

?Q-3. Is your state building capability to response to a significant cyber incident outside of organic capabilities? For example, Michigan has created a volunteer force called the Michigan Cyber Civilian Corps. Maryland is looking to develop their state militia, the Maryland Defense Force.

- Do you have or are you planning to build capability like this in your state?
- If you have what is their strength?
- Have they been used?

Indiana is looking to build additional capability within the Indiana State Police (ISP) by training ISP officers across the state in cyber. We are currently developing concepts and training programs to do this. The advantages we see in placing this in the ISP are legal. Unlike other constructs, the IPS is not limited by as many legal issues as National Guard assets or some other form of a volunteer force.

?Q-4: Are there capabilities identified within your state that you are considering filling with National Guard personnel?

- Are there other areas that you are investigating to support the state's cyber readiness?
- Have you developed working partnerships with Federal/State agencies and what engagements are you using to foster these relationships.

One gap identified in our research is the lack of a cyber analyst in the State's Fusion Center. We are conducting a business case analysis and plan on seeking State funding to fill this capability gap.

California:

Cybersecurity Task Force
The California Cybersecurity Task Force is responsible for identifying, acquiring and establishing funding mechanisms to enhance cybersecurity efforts; promoting actions to enhance cybersecurity; growing the cybersecurity workforce; developing public education; facilitating economic development by promoting a cyber-safe location for businesses and consumers; enhancing cyber emergency preparedness and response; identifying, understanding and sharing cyber threat information; mitigating the cyber risk; and building a comprehensive digital forensics and cyber investigative capability. The task force serves as an advisory body to senior administration officials in matters related to cybersecurity.

NG POC - LTC Jim Parsons, James.L.Parsons@cnd.ca.gov

Q-1 "Assessments/PEN Testing" - CA uses a full time CND-T team funded the State using SAD funding. State law, CA Assembly Bill No 670, which has a standing Network Defense team made up of National Guardsmen paid by state funds that is authorized by the bill to conduct network assessments among other cyber related duties of state agencies and then reimbursed by the agency assessed. CA law requires state agencies to have tests completed every two years and to use state CND-T. Team schedule is full year round.

Q-2 "State Cyber Response Plan" - The state is looking for leadership to oversee a Volunteer Civilian Cyber Force. Incorporates the use of CANG into state response.

Q-3 "State Capacity Building" -

Q-4 "State NG Partnering" -

Georgia:

POC - COL David S. Allen, GAARNG (US) <david.s.allen1.mil@mail.mil>

LTC Anthony (Tony) B. Poole, DCoS, GAARNG (US) <anthony.b.poole.mil@mail.mil>

Q-1 "Assessments/PEN Testing" - In Georgia, we are taking steps to assist the Georgia Technology Authority and Department of Accounts/Audits with vulnerability assessments. These activities will be a mix of SAD/IRT depending on the scope of the work per Deputy Secretary of Defense Policy memorandum 16-002. We are also in preliminary discussions with the Department of Driver Services for PEN testing of their POS system. Our focus currently is with general state agency cyber defense and the energy sector. We are developing plans to exercise the DSCA cyber response process within the next 12-18 months. Our TTPs outside of general cyber incident response are still in development.

Q-2 "State Cyber Response Plan" - The GAARNG has developed a CONPLAN for Cyber Incident Response within the state. This plan was originally developed and published in FY16. This plan provides guidance should the state request support due to a significant cyber incident. The GAARNG is not currently involved in the initial decision making process during such an event. We are developing plans to exercise the DSCA cyber response process within the next 12-18 months. Portions of this plan were exercised during our FY17 Vigilant Guard exercise in conjunction with Title 10 members of the Fort Gordon Cyber Protection Brigade.

Q-3 "State Capacity Building" - The GAARNG is not building a similar capability at this time. We are pursuing initial conversations with certain Cyber Academic Centers of Excellence that may lead to development of a similar capability.

Q-4 "State NG Partnering" - The GAARNG has developed relationships with Federal/State/Local and commercial entities. We currently meet monthly for a cybersecurity working group that includes DHS, FEMA, Secret Service, ICE, Georgia Technology Authority (GTA), and Georgia Bureau of Investigation (GBI). Commercial partners include Metro Atlanta Rapid Transit Authority (MARTA) and Southern Company/Georgia Power. This meeting provides intelligence sharing across the organizations and assists with exercise participation and planning for real-world events. Current efforts include planning for a DSCA Cyber tabletop and the 2019 Super Bowl.

Indiana:

Executive Order: Executive Council on Cybersecurity
This executive order establishes a public-private partnership charged with enhancing Indiana's ability to prevent, respond to and recover from all types of cybersecurity issues, including attacks. The council consists of the homeland security department, CIO, attorney general, adjutant general, state police superintendent, utility regulatory commission chair and others.

NG POC - Mr. David Tygart, Chief Defensive Cyber Programs, david.b.tygart.civ@mail.mil, (317) 247-3323

Assessments/PEN Testing - No test conducted to date. The Indiana National Guards is developing capability and processes to conducted penetration assessments that supports both Internal training objectives and support to State and local government agencies of Indiana thru the Governor's Indiana Executive Council on Cybersecurity. Initially these test will not be to the depth that DHS National Cybersecurity Assessments and Technical Services team (NCATS) conducts but anticipate refining processes and expanding offerings over time. Currently the majority of our assets are deployed and equipment to conduct such testing is in procurement. We plan to have a limited capability in the next 90 days and a robust capability in 180 days.

Q-1 "Assessments/PEN Testing" - We will look at SAD funding and also explore the use of a DoD program called Individual Readiness Training (IRT) that allows use of DOD assets in title 32 status.

Q-2 "State Cyber Response Plan" - Although State legislation was introduced to develop a Volunteer Cyber force construct in Indiana it did not get past committee. Indiana is taking an alternative approach and working to develop a Cyber Taskforce Enforcement Training program to train members of the Indiana State police across the state. The unique advantage to this approach is that it eliminates legal issues other states are facing with a volunteer cyber force. The Indiana will work closely with and augment these teams in the future.

Q-3 "State Capacity Building" - .

State Cyber Plan - Currently in draft form. This plan will creates the Indiana Cyber Advisory Group (CAG). The CAG is a flexible body of emergency management professionals and subject-matter experts that can be scaled to individual cyber incidents. The National Guard is a foundational member.
Q-4 "State NG Partnering" -

Louisiana:

POC - LTC Stephen Durel, Deputy J6, 504-278-8051, stephen.l.durel.mil@mail.mil

Q-1 "Assessments/PEN Testing" - Currently in Louisiana we are not conducting vulnerability however; we are exploring the options with our current state government.

Q-2 "State Cyber Response Plan" - In Louisiana the Governor and TAG have dedicated state and Guard resources to the Cyber defense effort. In December 2017 the Louisiana Governor had formed a 15 member Cyber commission to address the growing Cyber threat to our state at all levels. Additionally the governor in February 2017 tasked his staff, GOHSEP (Governor's Office of Homeland security and preparedness) and the Guard to develop an ESF (Emergency Support Function) -17 that is be specific cyber. Included with this ESF is a Cyber response plan that the Guard help to draft. Currently the Guard with other state and federal agencies is planning a Cyber TTX that will take place in 2019.

Q-3 "State Capacity Building" - Louisiana formed an ad-hoc Cyber team called CDIRT (Cyber Defense Incident Response Team) Louisiana's TAG guidance was to form a Cyber team made up of volunteers from Air and Army DRU's that had IT and Cyber back grounds. The team was formed back in 2013 and conducts quarterly training events at joint Cyber range which LSU manages in a Cyber lab that both GUARD and LSU partnered and built. Once Louisiana was awarded the CPT we filled the positions with CDIRT members which deployed the past March. We are currently leaning forward by rebuilding our cyber team a surge capacity refilling our CDIRT ranks with the next wave of Cyber defenders. Future opportunities.

Q-4 "State NG Partnering" -

We currently we are trying to put intelligence folks into the state fusion center (LA-SAFE) Louisiana state and analytical fusion exchange.
The cyber commission that Louisiana's governor had formed is currently forming sub-committees to identify various cyber issues to include defining each state and federal organizations cyber capabilities' and conducting GAP analysis to fill those needs.
Louisiana has developed several working relationships with both State and Federal partners. The Guard works with GOHSEP in cyber planning, training and conceptual theories. The Guard works with DoA in Cyber planning and execution to include being Co-Leads of the governors proposed Cyber emergency support function (ESF-17). We also work with our state Fusion center (LA-SAFE) with Cyber awareness and information sharing. Members of the CPT and CDIRT work with our federal partners (DHS and FBI) and are members of the FBI Cyber Task Force.

Maryland:

Legislation: Maryland Cybersecurity Council
The council, created in 2015, is responsible for reviewing and conducting risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber-attacks and need the most enhanced cybersecurity measures; assisting private sector cybersecurity businesses in adopting, adapting and implementing NIST framework; recommending a comprehensive state strategic plan to ensure a coordinated and adaptable response to and recovery from cybersecurity attacks; and other responsibilities. The council is made up of the attorney general (chair), secretary of information technology, secretary of the state police, secretary of business and economic development, adjutant general, executive director of the office of homeland security, the executive director of the development corporation and others.

NG POC - MATTHEW D. DINMORE, Col, MDANG, Joint Staff/J6 Maryland National Guard
matthew.d.dinmore.mil@mail.mil <mailto:matthew.d.dinmore.mil@mail.mil> (443) 927-4011

Q-1 "Assessments/PEN Testing" - One test conducted, future tests planned on a quarterly basis and dependent on ability to sustain these missions. Focus on State agencies. No testing with State critical Infrastructure entities planned currently but it's a high-interest item. Relooking a "joint training" program with both components, state entities, law enforcement, etc. based on several demand signals from state leadership, our state department of IT, and others. TTPs and CONOPS in very rough draft form and will be refined over time. Participation in GRIDEx and other ICS/SCADA activities over the past few years, basic skills and processes developed, future efforts will tie to more engagements. Over the last year+ we've worked with our Maryland Emergency Management Agency (MEMA), Department of IT, and other agencies to build the cyber incident response plan. Version 1 was signed out last year and we exercised it in CYBER PRELUDE.

Q-2 "State Cyber Response Plan" - We have a volunteer cyber unit as part of our state militia, the Maryland Defense Force. The MDDF is part of the military department, so reports to TAG, but falls outside T32 "limits." We integrate the cyber unit into our overall response plan through the joint staff. MD is researching volunteer cyber capabilities, inspired by Estonia's cyber defense league http://www.kaitseliit.ee/en/cyber-unit

Q-3 "State Capacity Building" -
Q-4 "State NG Partnering" -

Michigan:

POC - Matthew LoCricchio, LoCricchioM@michigan.gov (PEN); Dr. Ray Davidson, Office of the CSO Michigan Cyber Civilian Corps, 269.929.2554, DavidsonR5@michigan.gov

Q-1 "Assessments/PEN Testing" - Not being conducting currently but in the planning stages.

Q-2 "State Cyber Response Plan" - MI establish by law a volunteer civilian cyber response force. Costs to oversee the force is estimated at $700k per year and they have 30 personnel signed up to date. They have not been employed as of yet due to unforeseen legal issues. We are also initially limiting ourselves to businesses in the health/medical, educational, and financial sectors, in addition to government entities.

Q-3 "State Capacity Building" - Yes approved plan on the shelf.

Q-4 "State NG Partnering" -

Minnesota:

POC - COL Rick Schute, J3, (651) 268-8931, richard.t.schute.mil@mail.mil

MAJ Chris Brossart, DJ6, christopher.p.brossart.mil@mail.mil

Q-1 "Assessments/PEN Testing" - No, we are not currently doing it, however, it would benefit the state agencies if we provided this type of service. Some work with Critical infrastructure with Excel Energy groups to better understand Industrial Control systems.

Q-2 "State Cyber Response Plan" - Unknown

Q-3 "State Capacity Building" - Not aware that this is happening although we do have the Minnesota Fusion Cell that does include cyber. Not to my knowledge; agency to consider would be Infragard.

Q-4 "State NG Partnering" - This should be answered by MN.IT. I would suggest filling a position in MN.IT, as well as potentially in the MN Fusion Center.

Mississippi:

POC - COL Joe Hargett, G3, Deputy Chief of Staff, (601) 313-6311,

Mccullouch, Murry Brent LTC USARMY NG MSARNG (US) <murry.b.mccullouch.mil@mail.mil>

MAJ Chris Brossart, DJ6, christopher.p.brossart.mil@mail.mil

Q-1 "Assessments/PEN Testing" - The MSNG Defensive Cyber Operations Element (DCOE) has conducted two vulnerability assessments for the Leake County school system and one assessment for the MS Secretary of State's Office. They have not conducted any penetration testing. For the Leake County school, the team conducted an external and internal IP scan. For the Secretary of State's office they conducted an external scan. Team members have been in a drilling status.

Q-2 "State Cyber Response Plan" - Mississippi does not have a Cyber Response Plan. We currently do not have any plans to exercise C2 with the state emergency management teams. The MSNG has had discussions with the MS Information Technology Services department on ways to integrate the Guard's cyber assets with the states' to develop a plan for emergency response.

Q-3 "State Capacity Building" - No.

Q-4 "State NG Partnering" - No.

Missouri:

POC - WO1 Kathleen D. Herrell, Cyber Operations Chief

Q-1 "Assessments/PEN Testing" - no due to legal issues. Passive using cap and rocket SM passive on network. Critical infrastructure not now, but starting to build relationship and trust. Part of Gold tm at CS18 to build trust. Funding is thru T32/CTAA with reservations. Looking for range options .and could use suggestion.

Q-2 "State Cyber Response Plan" - Yes and will exercise this summer.

Q-3 "State Capacity Building" -

Q-4 "State NG Partnering" -

Response Force Construct - looking at Militia discussions started but need legislation first.

Nebraska:

POC - COL Teegerstrom, Eric J, G3, eric.j.teegerstrom.mil@mail.mil

Q-1 "Assessments/PEN Testing" - Nebraska has not conducted any non DODIN assessments. We have been approached by a Public Power District to do a vulnerability assessment and participate in their incident response exercise. We are looking at using our CPT for a Site Assistance Visit as part of their

scheduled training plan on IDT status. Our TAG is working a contract with our University College of Law to review State Law and Federal Statutes about use of cyber. For instance, our State Law provides 'Good Samaritan' protections if a medic provides assistance to the best of their training. Hopefully our Law College will be able to clarify if that same State statue covers a CPT team responding to an event.

Q-2 "State Cyber Response Plan" - Nebraska State government does not specifically identify National Guard assets for cyber response. We do many exercises with our State, but none specifically focused on cyber.

Q-3 "State Capacity Building" - None. Many of our local colleges and universities are working on NSA accreditation and building classes to teach cyber in many areas (IT, Trades, Business) to increase the overall capacity of the Silicon Prairie and our TAG is very supportive of building partnerships with other agencies, however the Nebraska Military Department has not sought to build capacity in this manner.

Q-4 "State NG Partnering" - None at the G6 level.

New York:

POC - CW3 Thomas S. Fancher, NYARNG - Force Integration & Readiness Officer, thomas.s.fancher.mil@mail.mil, (518) 786-4590

Q-1 "Assessments/PEN Testing" - New York currently offers vulnerability assessments to critical infrastructure stakeholders, counties, governmental agencies, and local municipalities. The primary unit responsible for these engagements is the Cyber Support Element (CSE). The CSE is made up of National Guardsman working with the New York Division of Homeland Security and Emergency Services (DHSES). They have conducted 5 vulnerability assessments to date with 4 more scheduled through the summer. In addition, they conduct legislatively mandated site visits to critical infrastructure sites around the state and assist DHSES personnel in assessing the sites cyber security posture. New York Joint Forces Headquarters (JFHQ) G6 office is in the process of standing up a DCO-E to augment the states cyber incident response capabilities with validation at the Cyber Shield exercise next year.

Q-2 "State Cyber Response Plan" - Yes, the NYNG is referenced in the available force pool to the NYS CRP. From our discussions with NYS, NYNG would be used primarily to help maintain and restore (rebuild) functionality while a dedicated NYS CERT entity would conduct DCO. The planning and exercising is in its infancy.

Q-3 "State Capacity Building" - NY is concentrating on achieving functional readiness ratings for its recently activated CPT and reorganized DCOE. There is some capacity in the NY Guard (state militia) but it is not organized presently.

Q-4 "State NG Partnering" - Yes, NYNG has 6 Soldiers on State Active Duty with the NYSDHSES that conduct cyber vulnerability assessments for state and local governments. In addition, NYNG partners with the Army Cyber institute at West Point and the Center for Internet Security in Albany, NY on exercises and training.

North Dakota:

POC - COL James R. Olson, G3, james.r.olson.mil@mail.mil, W: 7013333090

Q-1 "Assessments/PEN Testing" - North Dakota is not conducting vulnerability assessments nor penetration testing with outside agencies. While we see this as a possible area of support for our mission partners, our cyber assets are currently not robust enough to accomplish this task. We continue to

participate in any and all exercises and Cyber working groups that are available to us, but the capabilities in this question will likely be more robust upon return of our Cyber Protection Team from its mobilization in early 2020. However, for this capability to exist in the future, it is paramount that our legal resources receive the training necessary for our forces to operate in this space.

Q-2 "State Cyber Response Plan" - Working - North Dakota is participating in a Cybersecurity Task Force called by the Director of Homeland Security. We are meeting with private business, utilities and State government to examine 15 of the 16 critical infrastructures (ND does not have nuclear). The end result of this Task Force is to develop an Incident Response Plan for North Dakota. We continue to feel our role largely amounts to a Coordinate Train Advise and Assist role as per the Secretary of Defense CTAA memo. We are working with colleges and universities to help shape cyber education, as well as assisting with general cyber education via conferences and workshops. Again in a CTAA role, our CPT has the capability to work with various entities to assist with cyber training and best business practices.

We don't have a Cyber Response Plan at this point, but do have an internal Incident Response Plan. We will be initiating work on a Cyber Annex to our All Hazard Response Plan in the near future.

Q-3 "State Capacity Building" - Interested - While we are not currently working to build this type of capability within North Dakota, it is certainly something in which we are interested. As per our response to Question #2, our work with the ND Task Force may lead to this type of capability once we have examined not only the capabilities within our state, but also the areas where our capabilities are not as robust.

Q-4 "State NG Partnering" - none - At this time, North Dakota is not looking to fill any other positions with National Guard personnel. Our State Fusion Center has a Cybersecurity analyst on staff from the North Dakota Information Technology Department. He is leading the Task Force mentioned in Question #2, and we have a very good relationship with him and his team. We continue to ensure our mission partners see the North Dakota National Guard as a viable resource like they would during any natural disaster. Our work in bringing together private and public educational institutions, private business and State and Federal resources has proven to be a very effective model.

Ohio:

POC - Mamula, Kevin T MAJ Cyber Lead, kevin.t.mamula.mil@mail.mil; Teri Williams , LTC J6/G6 / DoIM 346-7249 (614) 336-7249 teri.d.williams.mil@mail.mil

Q-1 "Assessments/PEN Testing" - The OHNG cyber team has conducted 12 assessments so far and plan to increase that number to 12-16 per year. Funding is provided by the State using SAD. Focus is on State cabinet/administrative departments currently. Other agencies can request support thru the governor's office. Actively conducting PEN testing, 12 so far, plan for 12-16 per year. Each test take 2 weeks and consist of Intel gathering, phishing e-mail and physical security breach attempts, followed by actual PEN testing and final report. No testing with State critical Infrastructure entities currently, plans underway to move towards this. TTPs and CONOPS in draft form.

Q-3 "State Capacity Building" -
Q-4 "State NG Partnering" -

Response Force Construct - OH is developing a Cyber Reserve that will work for the Governor and is nested under the TAG. This differs from the MI Civilian reserve force, unlike MI force that is managed by the state, the OH force will be managed by the TAG.

Q-2 "State Cyber Response Plan" -

Utah:

Legislation: Data Security Management Council
This law created the Data Security Management Council to review existing state government data security policies, assess ongoing risks to state government, create a method to notify state and local government entities of new risks, coordinate data breach simulation exercises and conduct other cybersecurity related activities. The council consists of the chief information officer, an individual appointed by the governor, an individual appointed by the speaker of the House of Representatives and the highest-ranking IT official from the judicial council, the board of regents, the office of education, the Utah College of Applied Technology, the state tax commission and the office of the attorney general.

NG POC - COL Paul S. Peters, G3/5/7
CW4 Rick Gardner, Deputy CIO / G6, Utah Army National Guard, O: 801-432-4111, C: 801-716-9129

Q-1 "Assessments/PEN Testing" - Utah has offered assessments as a "Force Package" that the governor could call on. As of today we have not conducted PEN testing or vulnerability assessments. It is anticipated that assessments would be in a SAD status. Both would be conducted by the DCOE.

Q-2 "State Cyber Response Plan" - Utah Department of Emergency Management (DEM) does have an All Hazards Response Plan with a Cyber Annex. The annex list and describes the UTNG DCOE as a resource for cyber incident response. We worked closely with DEM to develop the Annex and continue to coordinate with them and participate in table top exercise, in fact the next TTX is scheduled for 12 April. It will involve DHS, DEM, and Water/Waste Water Critical Infrastructure partners.

Q-3 "State Capacity Building" - Yes, Utah is in the exploratory phases of developing a Civilian Cyber Corps.

Q-4 "State NG Partnering" - Currently the DCOE collaborates and has working relationships with Utah Department of Technological Services, Utah DEM, State Attorney General's Office, Department of Homeland Services, FBI, local academia, and private sector partners.

Engagements include Key Leader engagements, regularly scheduled committee meetings, Table Top Exercises, Cyber Shield Exercise, training opportunities, JAG/Legal Counsel discussions, and consultation on cyber related activities.
NOTE: Has Cyber Forensics Team imbedded in its Counter Drug Program.

Virginia:

NG POC - LTC Terry Duran, Cyber Planner, (703) 995-7023

Q-1 "Assessments/PEN Testing" -

Response Force Construct -

http://vdf.virginia.gov/2016/12/19/vdf-serves-as-technical-lead-for-ongoing-cyber-assessment-mission/

Q-2 "State Cyber Response Plan" -

Q-3 "State Capacity Building" -

Q-4 "State NG Partnering" -

Washington State:

NG POC - Thomas A. Pries, Lt Col, WA ANG, J-36 Cyber Operations Plans, thomas.pries@us.af.mil
Comm: 253-982-1689

Q-1 "Assessments/PEN Testing" -

3/29/18 - No Pen tests on our side currently. We do offer this service and have done so in the past, but all of our customers are really more interested these days in a survey mission where we produce a relational model and Risk Mitigation Plan. Last mission was 10 guys for 3 weeks. Cost to customer was $70K, executed in SAD. Looking to do a repeat in T-32 next time around under CTAA, likely next winter some time if resources allow. Currently have one other mission in the planning stage that we'll execute in T-32 later this summer.

We have 2 CPT's in-state, and 3 additional Cyber to Physical System teams of 10 people each (currently manned at about 65%). Given this, we could comfortably support two missions per year and still meet our T-10 work load. We're definitely the anomaly though as I don't know of any other state that has that much resource to pull from. Our CPT's are heading into dwell over the next 18 months though so that'll limit availability somewhat.

11/1/17 - We are actively engaged in security assessments with both local government and private entities. However, our assessment method is a bit broader than just pen testing in that it follows the Air Force CPS (Cyber to Physical Systems) methodology. We offer a menu of options to our customers of which a traditional pen test is one item on the menu among others. Depending on what they feel best meets their goals we then scope the mission accordingly.

State National Guard Cyber Baseline

as of 27 April 2018

	POC	assesments past yr	Assesments planned / yr	Funding	Focus on (Gov Agencies)	Focus (Critical Infstr)	Note	CPT, CO BN pax	State Cyber Respons Plan	Response Force (Vol Civ other Cyber)
Alabama								11		
Alaska										
Arizona										
Arkansas								7		
California	LTC Jim Parsons	12	12	SAD	Yes	No	Full time team state funded with SAD	39	Yes	Civ Vol planned
Colorado								11		
Connecticut								9		
District of Columbia										
Delaware										
Florida										
Georgia	COL David Allen, G3 LTC Tony B. Poole, DCoS	0	Planning	SAD/IRT	Yes	Yes	Planning stage - Focus on state agency cyber defense and energy sector	39	Yes	None
Guam										
Hawaii										
Idaho										
Illinois								18		
Indiana	Mr. David Tygart, J36	0	6-12	SAD/IRT	Yes	Yes	IRT will br first Cyber request to NGB	11	Draft	ISP planed
Iowa	CPT Robert Randol									
Kansas										
Kentucky	SSG scott Paige, 175 CPT	0	0	NA	No	No	Focus on T10 mission	14		
Louisiana	LTC Stephen Durel, Deputy J6	0	0	NA	Future	No		18	Draft	AF#ARNG Response Team
Maine								11		
Maryland	COL Matthew Dinmore, J6	1	2	SAD			Vulnerability Assessment focus	39	Draft	Militia 20(+)
Massachusetts								53		
Michigan	Dr. Ray Davidson - Vol Cyber Force	No	No	NA	Yes	No		14	Yes	Civ Vol 30
Minnesota	COL Rick Schute, J3 MAJ Chris Brossart, DJ6	0	0	NA	NA	NA	Pending return of DCO/CPT leads	39	unk	unk
Mississippi	COL Joe Hargett, G3	2	unk	T32 Drill	Yes	Yes		7	No	None
Missouri	WO1 Kathleen D. Herrell, Cyber Op	2	2	SAD	Yes		Vulnerability Assessment focus, Full time tech March 2018	21		Militia (?)
Montana										
Nebraska	COL Teegerstrom, Eric J, G3	0	0	NA	NA	NA	Looking at using our CPT for a Site Assistance Visit	11	No	unk
Nevada										
New Hampshire								13		
New Jersey								14		
New Mexico										
New York	CW3 Thomas S. Fancher	6	10	SAD	Yes	Yes	6 full time SAD working with NYSDHSES	25	Yes	none
North Carolina										
North Dakota	COL James R. Olson, G3	0	0	NA	NA	NA	Not robust enough, after 2020. Legal unresolved	7	No	none
Ohio	MAJ Kevin Mamula, Cyber Lead	8	12-18	SAD/T32 CTAA	Yes	No	Focus on State Govrn Agencies PEN testing	14	Yes	Civ Vol planed
Oklahoma										
Oregon										
Pennsylvania										
Puerto Rico										
Rhode Island										
South Carolina								95		
South Dakota								7		
Tennessee								14		
Texas								14		
Utah	COL Paul S. Peters, G3/5/7 CW4 Rick Gardner D CIO / G6	0	0	SAD assumed	NA	NA	Cyber Forensics Tm in Counter Drug	14	Yes	Exploring Civilian Cyber Corps
Vermont								9		
Virginia	LTC Terry Duran, Cyber Planner	10+		SAD	Yes	Yes	Vulnerability Assessment focus state loc govn, schools. . .	271		VA Defense Force Militia
Virgin Islands										
Washington	Lt Col Thomas Pries, J-36	0	2	SAD/T32 CTAA	Yes	Yes	Focus on Risk Mitigation Plans not PEN	39 AF	Yes	

APPENDIX D.12
CYBER SHARING WORKING GROUP

CYBER SHARING WORKING GROUP STRATEGIC PLAN

Chair: Dewand Neely | Co-Chair: Ron Pelletier

September 2018
Indiana Executive Council on Cybersecurity

Cyber Sharing Working Group Plan

Contents

Committee Members **4**

Introduction **6**

Executive Summary **8**

Research **10**

Deliverable: Best Practices **14**

General Information 14

Implementation Plan 15

Evaluation Methodology 18

Deliverable: Cyber Sharing Maturity Model **20**

General Information 20

Implementation Plan 21

Evaluation Methodology 25

Deliverable: Inventory of Cyber Sharing Resources **27**

General Information 27

Implementation Plan 28

Evaluation Methodology 31

Deliverable: MS-ISAC Member Recruitment **33**

General Information 33

Implementation Plan 34

Evaluation Methodology 38

Deliverable: Secured Information Sharing Program **40**

General Information 40

Implementation Plan 41

Evaluation Methodology 46

Supporting Documentation **48**

IECC Cyber Sharing Working Group Inventory of Information Resources 49

Committee Members

Committee Members

Name	Organization	Working Group Positon	IECC Membership Type
Dewand Neely	Indiana Office of Technology	Chair	Voting
Tad Stahl	Indiana Office of Technology	Chair Proxy	Advisory
Ronald W.Pelletier	Pondurance	Co-Chair	Voting
Nick Sturgeon	CLA	Co-Chair Proxy	Advisory
Paul Baltzell	IEDC	Full time	Advisory
Franco Cappa	Purdue University	As needed	Advisory
Chris Carter	Indiana State Police	As needed	Advisory
Paul Dvorak	Secret Service	As needed	Non-Voting
Greg Hedrick	Purdue University	Full time	Voting
Owen LaChat	MutualBank	As needed	Voting
Benjamin Marrero	Ivy Tech	Full time	Advisory
Kim Milford	Indiana University	Full time	Advisory
Nicole Needham	Indiana Office of Technology	Full time	Advisory
Mitchell Parker	IU Health	As needed	Advisory
Stan Partlow	American Electric Power	As needed	Advisory
Chad Pollitt	Indiana University	Full time	Advisory
Joel Rasmus	Purdue University (CERIAS)	As needed	Advisory
Bryan Sacks	Indiana Office of Technology	As needed	Advisory
Michael Servas	MutualBank	As needed	Advisory
Dave (LT)Skalon	Indiana National Guard	As needed	Advisory
Darryl Togashi	Ivy Tech	As needed	Advisory
William Tucek	Navient	As needed	Advisory
Andrew VanZee	Indiana Hospital Association	As needed	Advisory
Brian Vitale	Notre Dame Federal Credit Union	Full time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - State cybersecurity plans
  - Magazine articles on state cyber sharing articles
  - Team member familiarity with resources
  - Applied experience by team members for their own operations, experience and networks with other organizations

- **Research Findings**
  - An inventory of cyber sharing resources of various sources
  - Articles depicting the various strategies used by state governments
  - Communication types produced by the Multi-State Information Sharing and Analysis Center (MS-ISAC) (a similar model for states that Indiana might learn from for counties)

- **Working Group Deliverables**
  - Best Practices
  - Cyber Sharing Maturity Model
  - Inventory of Cyber Sharing Resources
  - MS-ISAC Member Recruitment
  - Secured Information Sharing Program

Additional Notes
  - N/A

References
  - State cybersecurity plans (multiple)
  - Pew article - http://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf
  - ISC2 survey on cybersecurity from a Federal Executive perspective - https://www.isc2.org/-/media/ISC2/Documents/ISC2-Federal-Cyber-Survey-Report.ashx?la=en&hash=7AFB8F6E0A67C2D417D7031E17DF9E481DB21E20

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Over the last five years and before, there has been an emerging number of excellent cyber sharing resources. The process of finding information can be initially difficult and somethings the need and/or value of information is not recognized. If the need and/or desire for cyber information exists, the vast majority of it is available by searching websites and news articles.
    b. The numerous sources of information take various approaches to distributing material to their audiences. There are corporate sources providing the information as their primary product, there are technical sources providing cyber information as a value in the form of enhanced support to their customers, Information Sharing and Analysis Centers (ISAC) serving particular business sectors against common threats, and Fusion Centers sharing information to Federal sources and local law enforcement.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Filtering valuable information from the mountain of content available. The amount of information can be overwhelming and much of it is of no value to an organization. Identifying sources that provide pertinent information to a business function in an efficient manner is more difficult.
    b. Organization of cybersecurity maturity. Many agencies have not reached a maturity level with cybersecurity, or are not staffed to needed levels, to recognize and define the cyber information needed.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. To identify common needs that can be filled through economies of scale and facilitated by the Council.
    b. An understanding of where various entities in Indiana, public and private, are underserved and why they are underserved.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. A number of state entities fall under federal regulations (Internal Revenue Service (IRS), Health Insurance Portability and Accountability Act (HIPAA), Social Security Administration (SSA)). State law also directs Indiana citizens on appropriate behavior and incident response requirements.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Most states find themselves in a similar position as we do. Fusion Centers seem to be the most common form of information distribution, but are limited in audience and very specific with its content. ISACs, Information Sharing & Analysis Organizations (ISAO), and state-sponsored cyber sharing organizations are growing as vehicles to share to broader audiences.

6. **What research is out there to validate your group's preliminary deliverables? This could be Surveys, whitepapers, articles, books, etc.**
    a. A number of state cybersecurity plans were reviewed. Each state seems to have a slightly different focus or approach, but also a lot of commonalities. This document from Pell discusses seven states' information sharing (among other aspects of their cybersecurity efforts). http://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Most states and organizations look internally. Some states try to leverage their state, local, tribal and territorial (SLTT) relationships. ISACs and Fusion Centers work to develop economies of scales. For the most part, cybersecurity training and preparedness is left to individual organizations.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Success will be identifying the information available and matching it with the information needed, adding any needed value that exists, and facilitating the exchange of information between all organizations. This could be in the form of digital information, presentations, training, etc. Digital information would be the general content, threat information, advisories, vulnerabilities, etc. that entities should be aware of.
    b. Success will be finding ways of advancing cybersecurity maturity for individual SLTT units. Often one at a time or in small groups sharing similar challenges. The difficulty is having current and useful resources/services that will be able to help with these challenges in a timely manner.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. This will take some investigation. There could be opportunities for general cyber information to broad audiences/communications or specific information/communications for narrower audiences. There are other opportunities to make current communications, resources, and forums known to more audiences that could benefit from the information that already exists.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. Unknown.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. A vibrant and energetic cyber community, complete with sharing opportunities and effective communications, would be an attractive and prominent bullet point in attracting new opportunities.

12. What are your communication protocols in a cyber emergency?

a. The communication protocols vary with each communications channel. The State of Indiana communicates issues of concern with the MS-ISAC and other parties as needed. The Indiana Intelligence Fusion Center (IIFC) communicates with federal and local sources. The Indiana Information Sharing and Analysis Center (IN-ISAC) works with organizations, to include elections, state agencies, K-12, on an ad hoc basis as well as publishing a weekly security brief for the Executive Branch and a monthly newsletter for the general public.

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. The goal of the Cyber Sharing Working Group is to determine what are the best practices that should be used across the sectors of Indiana. There is a number of good information gathering organizations that effectively communicate with their constituencies. Some organizations are underserved which provides an opportunity to deliver solutions of real value.

Deliverable: Best Practices

Deliverable: Best Practices

General Information

1. **What is the deliverable?**
   a. A list of cyber sharing best practices

2. **What is the status of this deliverable?**
   a. In progress; 75% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☒ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Provide a recommendation of best practices for information sharing in the state. This will also provide a common set of terms that will make it easier to communicate effectively.

6. **What metric or measurement will be used to define success?**
   a. The adoption of the standards and best practices throughout the State of Indiana.

7. **What year will the deliverable be completed?**
   a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. The Public and Private Sectors

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Not applicable.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Not applicable.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Not applicable.

12. **Who should be main lead of this deliverable?**
    a. Cyber Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. None

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop List	Nick Sturgeon	100%	March 2018	
Review with the Cyber Sharing Working Group	Cyber Sharing Working Group	100%	May 2018	
Present update on the deliverable	IECC	100%	April 27, 2018	
Determine the home for the list and review with the working group	Cybersecurity Program Director and Cyber Sharing Working Group	100%	August 2018	
Finalize list	Cyber Sharing Working Group	50%	January 2019	
Publish the list and move to a maintenance mode	Cyber Sharing Working Group	0%	January 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. It will help businesses and citizens by creating and centralizing a list of best cybersecurity practices.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This will help increase knowledge of cybersecurity best practices to Indiana businesses and citizens. No real cost associated with this deliverable. With the adoption of these best practices, businesses and citizens will reduce the overall cybersecurity risk profile of the entire state.

19. What is the risk or cost of not completing this deliverable?

a. No risk, will only cost time to make the updates to the Indiana Cybersecurity website.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Initial metrics will be based around unique website visits and total site visits. Additional metrics will be around capturing data to see if these best practices are being implemented.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. [No Response]

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None as of now.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. The only people contacted to this point are those within the Cyber Sharing Working Group.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Sector partners, local government, state agencies, businesses and their associations, the general public

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC Cyber Sharing Working Group will create a list of best practices by January 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Sharing Maturity Model

Deliverable: Cyber Sharing Maturity Model

General Information

1. **What is the deliverable?**
   a. Cyber Sharing Maturity Model

2. **What is the status of this deliverable?**
   a. In progress; 50% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Creation of a maturity model that businesses and governments can self-assess and use links/info provided to increase their cyber maturity.

6. **What metric or measurement will be used to define success?**
   a. Completion of product, sample feedback from a variety of stakeholders, and a number of downloads of the model from the cyber hub.

7. **What year will the deliverable be completed?**
   a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Businesses and government

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Strategic Resources Working Group and the voting members of the IECC.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. N/A

12. **Who should be main lead of this deliverable?**
    a. Cyber Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Measuring of the success of the model and keeping the model simple enough for all to use.

Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Draft up model	Cybersecurity Program Director	100%	March 2018	
Review and develop model	Cyber Sharing Working Group, Strategic Resources Working Group, Indiana University Team	100%	April 2018	
Present model for feedback from Council	IECC	100%	April 27, 2018	
Make edits and design	Cybersecurity Program Director and Cyber Sharing Working Group	50%	January 2019	
Finalize Model	Cyber Sharing Working Group	0%	February 2019	
Incorporate model into IECC PR and Communications Plan	Public Awareness and Training Working Group	0%	March 2019	
Distribute to stakeholders	IECC and partners	0%	June 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The Cyber Sharing Maturity Model will provide all those who use it, especially local government, K-12 schools, and small businesses with a starting point to begin understanding the many resources around cyber threat sharing and education.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. By further educating those who would like to increase their cybersecurity levels, it will help reduce their cybersecurity risks and impact because they may be better prepared for a cyber event.

19. What is the risk or cost of not completing this deliverable?

a. As of now, many are confused by the many choices with cyber sharing and threat resources. Because it can be overwhelming, many do not move their cybersecurity level.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The completion of the model will be one output measure of success. This model is to be used by local governments, businesses, and educators in Indiana and them finding value in it will be another measure of success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. While there are many states that have cyber sharing resource pages, we were not able to find a similar maturing model

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None as of now.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Indiana University who provided the idea of a cyber sharing maturity model and are partners of this deliverable.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Sector partners, local government, state agencies, businesses and their associations, general public

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC will develop Indiana's first cyber sharing maturity model by February 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC will distribute Indiana's first cyber sharing maturity model to critical infrastructures through ninety percent of Indiana associations by June 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Inventory of Cyber Sharing Resources

Deliverable: Inventory of Cyber Sharing Resources

General Information

1. **What is the deliverable?**
   a. An inventory of resources assembled by the Cyber Sharing Working Group.

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. The inventory serves as a resource for those needing trusted and vetted cyber information.

6. **What metric or measurement will be used to define success?**
   a. We envision this being static content on an IECC web page. One metric is the number of hits, though this will not likely drive huge web traffic. It could be of exceptional value to those needing information, especially those just ramping up their security programs.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Business, government and possibly citizens.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. There is likely some overlap, but the accumulation of the inventory was straightforward. Keeping the list current will require little maintenance and any overlap would be inconsequential.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. This work is complete.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Not applicable.

12. **Who should be main lead of this deliverable?**
    a. Cyber Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Reaching the potential audiences effectively. Having the ability to share the value of the products.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
List developed	Cybersecurity Program Director	100%	November 2017	Ongoing only in that additional resources can be added
Review and develop model	Cyber Sharing Working Group	100%	November 2017	
Present model for feedback from Council	IECC	100%	December 2017	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. It is part of a library of resources that could be used by those needing cybersecurity guidance.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Provides information resources that will assist those needing cyber information.

19. What is the risk or cost of not completing this deliverable?

a. No risk, but a resource that could be very valuable.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The list could be very valuable to those that visit the library of resources. It will be hard to measure the value of coming to a trusted source and viewing the information. You could measure web hits on the document, but the value from any visit will be hard to measure.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

b. **If Yes, please list states/jurisdictions**

i. A number of states have lists of resources. Michigan is one example, but there are other examples as well. The types of resources in their libraries vary.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. There are many states that do not have a list of resources such as this. Cybersecurity and outreach from states to citizens, businesses, etc. are widely varied in both content and delivery mechanisms.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. IN-ISAC, Indiana Office of Technology (IOT)

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Sector partners, local government, state agencies, businesses, and their associations, as well as the general public

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC Cyber Sharing Working Group will complete an inventory of cyber sharing resources by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: MS-ISAC Member Recruitment

Deliverable: MS-ISAC Member Recruitment

General Information

1. **What is the deliverable?**
    a. MS-ISAC is a resource delivering a broad range of information to the State of Indiana. This includes vulnerability notifications, threat notifications, and other information including a monthly conference call. The Cyber Sharing group, through the efforts of the IN-ISAC, plans to push enrollment in the MS-ISAC. Education and Local government working groups may be able to assist with this deliverable.

2. **What is the status of this deliverable?**
    a. In-progress; 50% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Better cybersecurity information to a broad range of schools and local governments that are underserved.

6. **What metric or measurement will be used to define success**?
    a. Number of Indiana SLTT and K-12 schools signed up for the MS-ISAC.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. SLTT and K-12 organizations signing up for the information.

9. **Which state or federal resources or programs overlap with this deliverable**?
    a. MS-ISAC produces quality information in a variety of formats. This information is valuable and vetted.

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Getting the word out to SLTT and K-12 would be very helpful.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Those that can help with the drive to get SLTT and K-12 organizations to join MS-ISAC.

12. **Who should be main lead of this deliverable?**
    a. Tad Stahl

13. **What are the expected challenges to completing this deliverable?**
    a. Reaching the potential audiences effectively and having the ability to share the value of the products.

Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop Outreach plan	IN-ISAC Manager	100%	2018	
Implement plan and tactics	IN-ISAC Manager	25%	June 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Getting good, current and vetted cyber threat, advisory, and awareness materials to those subscribed on a regular basis.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Through better information to those involved in the daily security operations of an organization.

19. What is the risk or cost of not completing this deliverable?

a. There are many state institutions that could benefit from the federally funded service. This service is also free to SLTT and schools. Any costs for MS-ISAC would go unrealized.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Difficult to gauge the value from participants. It can be measured in the increased numbers using MS-ISAC.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. All states subscribed to the MS-ISAC newsletter.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None as of now.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. IN-ISAC
27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. Locals and Schools

Communications

---

28. **Once completed, which stakeholders need to be informed about the deliverable**?
    a. SLTT and schools.

29. **Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?**
    a. Yes

30. **What are other public relations and/or marketing considerations to be noted?**
    a. None as of now.

Evaluation Methodology

Objective 1: Increase Indiana MS-ISAC membership by twenty-five percent by June 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Secured Information Sharing Program

Deliverable: Secured Information Sharing Program

General Information

1. **What is the deliverable?**
   a. Secured Information Sharing Program

2. **What is the status of this deliverable?**
   a. In-progress; 75%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☒ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Provide a secure and trusted statewide information sharing platform.

6. **What metric or measurement will be used to define success?**
   a. Participation in the program by the private sector.

7. **What year will the deliverable be completed?**
   a. 2019

8. **Who or what entities will benefit from the deliverable?**
   a. Public and private sector

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. U.S. Department of Homeland Security's (US-DHS) Cyber Information Security Collaboration Program (CISCP), Enhanced Security Services (ECS) and Automate Indicator Sharing (AIS), MS-ISAC, and IN-ISAC.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Strategic Resource Working Group, Pre- thru Post- Incident Working Group

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. US-DHS, Indiana Department of Homeland Security (IDHS), IIFC, IN-ISAC, and Indiana State Police (ISP).

12. **Who should be main lead of this deliverable?**
    a. Cyber Sharing Working Group.

13. **What are the expected challenges to completing this deliverable?**
    a. The vetting process through US-DHS, participation from the private sector.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop Draft	Nick Sturgeon	100%	March 2018	
Review with the Cyber Sharing Working Group	Cyber Sharing Working Group, Strategic Resources Working Group, Indiana University Team	100%	March 2018	
Present program for feedback from Council	IECC	100%	April 2018	
Make edits to the program	Cybersecurity Program Director and Cyber Sharing Working Group	50%	March 2019	
Meet with ISP, IIFC, IDHS and US-DHS	Public Sector Working Group.	0	May 2019	
Make final edits and conduct the final review with the Cyber Sharing Working Group	Cyber Sharing Working Group	0	July 2019	
Deliver final product	Cyber Sharing Working Group	0	August 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
TBD	TBD	TBD	TBD	TBD	More conversation needs to be had on determining the work effort to manage and maintain this program

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
TBD	TBD	TBD	TDB	TBD	TBD	More conversation needs to be had on determining the work effort to manage and maintain this program. There is the potential for needing IT infrastructure for this program.

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. With the State of Indiana providing a secured cyber threat information sharing service for companies that want to share with the Federal Government. The State and the companies involved will be in a position to gain a clearer common operating picture. Another benefit for those involved is that these programs provide some limited liability protections.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This would also provide incentive for private sector businesses to share information with both the State and Federal Governments without fear of liability repercussions.

19. What is the risk or cost of not completing this deliverable?

a. There are potential liability risks at the state level with private sector and public sector sharing information. There are risks of the Cybersecurity Information Sharing Act (CISA) if information is not shared according to the guidelines needed to meet the liability protections laid out by CISA.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Initial metrics will be based on the number of private sector entities participating in the program and the level of their participation.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. This program will incorporate programs offered by the US-DHS.

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. No
    b. **If Yes, please list states/jurisdictions**
        i. We are unaware of any other state jurisdiction that has this exact program. There are states that have different sharing capabilities and maturity levels.

Other Implementation Factors

---

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. The biggest factor that would negatively impact this program will be the lack of acceptance and participation by the private sector and the buy-in from ISP, IIFC, US-DHS and IDHS. There could be kick-back from programs like InfraGard

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. Yes
    b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
        i. There may need to be changes to state law similar to the protections from Freedom of Information Act (FOIA) request that Michigan, House Bill 4973, signed into law in March 2018.

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. This program will require support from the ISP, IIFC, IDHS, US-DHS and private sector.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. No one at this time.

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. All

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Sector partners, local government, state agencies, businesses and their associations, general public

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC Cyber Sharing Working Group will develop a Secured Information Sharing Program by July 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Cyber Sharing Working Group will launch a Security Information Sharing Program by August 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- IECC Cyber Sharing Working Group Inventory of Information Resources

IECC Cyber Sharing Working Group

Inventory of Information Resources

August 2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Inventory of Information Resources

Type of Information	Source	Interval	Audience	Notes	URL
On-line webinars	MS-ISAC	Frequent, regular	All members		https://www.cisecurity.org/ms-isac/
Monthly newsletter	MS-ISAC	Monthly	All members		https://www.cisecurity.org/ms-isac/
Advisories -UFOUO	MS-ISAC	Frequent, regular	All members	Distributes from multiple sources (DHS, FBI)	https://www.cisecurity.org/ms-isac/
SOC advisories	MS-ISAC	Frequent, regular	State of IN	We are a customer, data could be scrubbed and shared	https://www.cisecurity.org/ms-isac/
Election Communications	MS-ISAC	Frequent, regular	Sec of State	Multiple comms type, election specific	https://www.cisecurity.org/ms-isac/
News	SANS	Weekly	Subscribers	Informational	https://www.sans.org/
Advisories -UFOUO	DHS	Frequent, regular	All states		https://www.dhs.gov/
Advisories	DHS	Infrequent	All states		https://www.dhs.gov/
Advisories	FBI (IC-3)	Infrequent	All states		https://www.fbi.gov/
Advisories	McAfee	Frequent, regular	Customers	Tend to focus on McAfee products, occasional acute threats	https://www.mcafee.com/en-us/index.html
	Shadowserver.org				https://www.shadowserver.org/wiki/
	FS-ISAC				https://www.fsisac.com/
	REN-ISAC				https://www.ren-isac.net/
	Open DNS				https://www.opendns.com/
	NH-ISAC				https://nhisac.org/
Advisories	FinCEN (Financial Crimes Enforement Network)				https://www.fincen.gov/
	FBI InfraGard		Members	Similar to FS-ISAC Alerts	https://www.infragard.org/
	US-CERT		Subscribers	General - Across all sectors / industries	https://www.us-cert.gov/
	Secret Service		Subscribers	General - Across all sectors / industries	https://www.secretservice.gov/
	Consumer Financial Protection Bureau		Subscribers	Bank / Non-Bank focused	https://www.consumerfinance.gov/
	Office of Comptroller of Currency		Subscribers	Bank / Non-Bank focused	https://www.occ.treas.gov/
	Federal Reserve Bank		Subscribers	Bank focused	https://www.federalreserve.gov/
	Federal Deposit Insurance Corporation		Subscribers	Bank focused	https://www.fdic.gov/
	National Credit Union Administration		Subscribers	Credit Union focused	https://www.ncua.gov/Pages/default.aspx
	Federal Financial Institutions Examination Council		Subscribers	Bank / Credit Union focused	https://www.ffiec.gov/
	Krebs-on-Security (Blog)		Subscribers	General - Across all sectors / industries	https://krebsonsecurity.com/
	National Association of Federally-Insured Credit Unions		Subscribers	Credit Union focused	https://www.nafcu.org/
	Indiana Credit Union League		Subscribers	Credit Union focused	https://www.icul.org/Pages/default.aspx
	Credit Union National Association		Subscribers	Credit Union focused	https://www.cuna.org/

APPENDIX D.13
CYBER SUMMIT WORKING GROUP

CYBER SUMMIT WORKING GROUP STRATEGIC PLAN

Chair: Chetrice Mosley | Co-Chair: Doug Rapp

September 2018
Indiana Executive Council on Cybersecurity

Cyber Summit Working Group Plan

Contents

Committee Members **4**

Introduction **6**

Executive Summary **8**

Research **10**

Deliverable: Cybertech Midwest **13**

General information 13

Implementation Plan 14

Evaluation Methodology 18

Supporting Documentation **20**

IECC Cyber Summit Working Group Cybertech Midwest October 2018 Brochure 21

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Chetrice Mosley	State of Indiana	Cybersecurity Program Director	Chair – Full Time	IECC Director
Doug Rapp	CLA	President	Co-Chair Full Time	Advisory
Steve Scofes	Scofes Consulting	President	Full Time	Advisory
Graig Fairmouth	Scofes Consulting	Partner	Full Time	Advisory
Brian O'Hara	InfraGard	Past - President	As Needed	Advisory
Chris Collins	InfraGard	President	Full Time	Advisory
Tom Gorup	Rook Security	Director of Security Operations	As Needed	Advisory
Chuck McCormick	ESO Communications	Solutions Engineer	As Needed	Advisory
Chad Pittman	Purdue Research Foundation	VP	As Needed	Advisory
Graig Lubsen	IOT	Communications Director	Full Time	Advisory
Joel Rasmus	Purdue	CERIAS Director	As Needed	Advisory
Diana Williams	Project Brilliant	Director	As Needed	Advisory
Julia Kraut	Cybertech	Events Director	As Needed	Contributing

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Collect initial feedback from cyber experts, states, and vendors for what would be valuable in a conference
  - National Governor's Association 2018 list of highlighted state conferences
  - Best practice research of cyber conferences
  - Listing of 2017 past conferences and rankings
  - Survey to Council for topics – upcoming
  - Reviewed materials of an award-winning state conference (Tax Symposium 2013)

- **Research Findings**
  - Initial discussions suggest that there is a great interest in Indiana leading the cybersecurity effort, including holding a state-wide conference.
  - In 2018, there are about 200 cybersecurity conferences being held by other states according to the National Governor's Association.
  - No other cybersecurity conference led by the State of Indiana has yet occurred.
  - Multiple sectors, academia, and military branches have conducted cyber-related education and training, along with preparatory cybersecurity workshops and conferences.

- **Working Group Deliverable**
  - Cybertech Midwest

- **Additional Notes**
  - N/A

- **References**
  - Comprehensive national and international list of cybersecurity conferences: https://infosec-conferences.com/
  - "The Top 50 Must-Attend Information Security Conferences": https://digitalguardian.com/blog/top-50-must-attend-information-security-conferences
  - Putting on Conferences – Best Practices:
    - https://www.smartmeetings.com/events/97322/planners-reveal-best-practices-for-how-to-plan-a-conference
    - https://www.semrush.com/blog/top-5-conference-best-practices/
    - https://medium.com/tedx-experience/how-to-organize-a-conference-567fb50ccdbd
  - Cybertech: https://www.cybertechisrael.com/

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. No other cybersecurity conference led by the State of Indiana has yet occurred.
    b. Multiple sectors, academia, and military branches have conducted cyber-related education and training, along with preparatory cybersecurity workshops and conferences.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Lack of education and knowledge of how cybersecurity affects everyone.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. There is a need for a state-sponsored cyber conference to assist in moving Indiana to the Next Level in cybersecurity.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. N/A

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. National Governors' Association experience with other state's conferences and their own.
    b. InfoSec Cybersecurity Conference Website Research.
    c. Best practices of conferences research.
    d. Feedback and lessons learned from other entities who have put on a cybersecurity conference in Indiana.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. Needs from stakeholders, councils, committees, and working groups.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Multiple sectors, academia, and military branches have conducted cyber-related education and training, along with preparatory cybersecurity workshops and conferences.
8. **What does success look like for your area in one year, three years, and five years?**
    a. Over the next year, the IECC will hold the first cybersecurity statewide conference that will be useful to the attendees, speakers, and vendors.
    b. Future cybersecurity conferences will need to align with the needs of the state and recommendations of the IECC.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. Comprehensive communication marketing plan to promote the cybersecurity conference throughout the State.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. N/A

11. **What do we need to do to attract cyber companies to Indiana?**
    a. N/A

12. **What are your communication protocols in a cyber emergency?**
    a. N/A

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. N/A

Deliverable: Cybertech Midwest

Deliverable: Cybertech Midwest

General information

1. **What is the deliverable?**
    a. Hold Cybertech Midwest, which is the state's first cybersecurity conference in 2018 with a sustainability model. See Supporting Document for Cybertech Midwest Brochure.

2. **What is the status of this deliverable?**
    a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☒ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Hold a successful cyber conference.

6. **What metric or measurement will be used to define success?**
    a. Meet income and attendee requirement for the conference.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. IECC, the general public, businesses, and government

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All as the program is developed.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IEDC and Cybertech

12. **Who should be main lead of this deliverable?**
    a. IECC Director

13. **What are the expected challenges to completing this deliverable?**
    a. Ensuring the income limit is met and a sustainability model is created

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort (3-year initiative)

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Select vendor	IECC Subcommittee	100%	NA	Cybertech
Select venue	IECC Subcommittee	100%	NA	JW Marriott
Finalize vendor contract	IEDC	100%	May 2018	
Finalize sponsorship details	Cybertech/Julia	100%	May 2018	
Meet initial sponsorship goal	Sponsor working group	0%	September 2018	
Draft schedule produced	IECC Subcommittee	100%	April 2018	
Content selected	IECC Subcommittee	100%	May -August 2018	
Speakers selected	IECC Subcommittee	85%	May -August 2018	
Website Launched	IECC Subcommittee	90%	May 2018	
Draft advertising campaign	IEDC/Subcommittee	85%	May -August 2018	
Meet registration goals	IECC Subcommittee	0%	September 2018	
Conduct final coordination	IECC Subcommittee	0%	September-October 2018	
Execute Summit	Cybertech/IECC	0%	October 2018	
Begin 2019 Planning	Cybertech/IECC		July 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. Seed funding secured by Indiana Economic Development Council (IEDC)
b. Marketing/Advertising support (from IECC partners and Cybertech)

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Provides a forum to conduct/highlight the work done by the IECC and the subcommittees.

18. **How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?**
    a. This event will provide education, training, and tools to reduce the largest risk surface area in Indiana.

19. **What is the risk or cost of not completing this deliverable?**
    a. The risk is that large areas of Indiana's economy remain unprotected.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Metrics of effectiveness will be determined by the subcommittee after further analysis. Standard metrics as to the success of the summit will include attendance, number of vendors, start-ups, and other participants.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. The Michigan summit can be used as a comparable as well as other Cybertech events.

22. **Are there comparable jurisdictions (e.g. other states) that do not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. No

Other Implementation Factors

---

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. Short timeline.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. It is the intent that the State provides initial seed funds for this initiative and Cybertech will have the responsibility to create a sustainability model in conjunction with the IECC.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. Governor's Office
    b. IEDC
    c. Additional subcommittees

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Formal public relations and marketing plan required.

Evaluation Methodology

Objective 1: IECC will secure a cybersecurity conference partner for three years by May 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: State of Indiana will hold its first statewide cybersecurity conference October 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Cybertech Midwest October 2018 Brochure

IECC Cyber Summit Working Group

Cybertech Midwest October 2018 Brochure

Summer 2018

CYBERTECH MIDWEST

OCTOBER 23, 2018 // JW MARRIOTT INDIANAPOLIS

KICK-OFF EVENT

Together with:

CYBERTECH MIDWEST

Indianapolis, Indiana

KICK-OFF EVENT: Oct. 23, 2018 // JW Marriott Indianapolis

CONFERENCE & EXHIBITION: Jul. 24-25, 2019

ORGANIZED BY

CYBERTECH

CYBERTECH MIDWEST

KICK-OFF EVENT

Together with:

OCTOBER 23, 2018 // JW MARRIOTT INDIANAPOLIS

Join Cybertech and the State of Indiana on **October 23, 2018** for the kick-off **Cybertech Midwest** event! Cybertech Midwest will return to Indiana the following summer on July 24-25, 2019.

Cybertech Midwest will host a thought-provoking conference and exhibition on global cyber threats, solutions, innovations and technologies.

Meet technology company executives, startups, government officials and contractors, investors, academics, media experts and other professionals changing the global cyber landscape.

Speakers and panelists will focus on the global cyber threat and strategies for meeting diverse challenges in sectors such as healthcare, utilities, small businesses and local government.

Topics will include:

>> **Emergency Management & Cyber Incident Response**

>> **Cybersecurity for Water Management**

>> **Securing the Cyber Workforce**

>> **Cybersecurity for Utilities**

>> **Cybermed: Cybersecurity for Healthcare**

>> **Scorecard: Cyber Readiness for Small Business & Local Government**

Cybertech Midwest will have a strong focus on networking, strengthening existing alliances and forming new ones, thanks to a B2B meetings platform. The conference will also highlight global and regional innovation with the renowned Cybertech Startup Pavilion, where cutting-edge companies can display their latest advances.

For more information or to register, visit us at midwest.cybertechconference.com

ORGANIZED BY

CYBERTECH

CYBERTECH AROUND THE WORLD

CYBERTECH TEL AVIV · **CYBERTECH** EUROPE, ROME · **CYBERTECH** SINGAPORE · **CYBERTECH** LOS ANGELES

UPCOMING CYBERTECH EVENTS

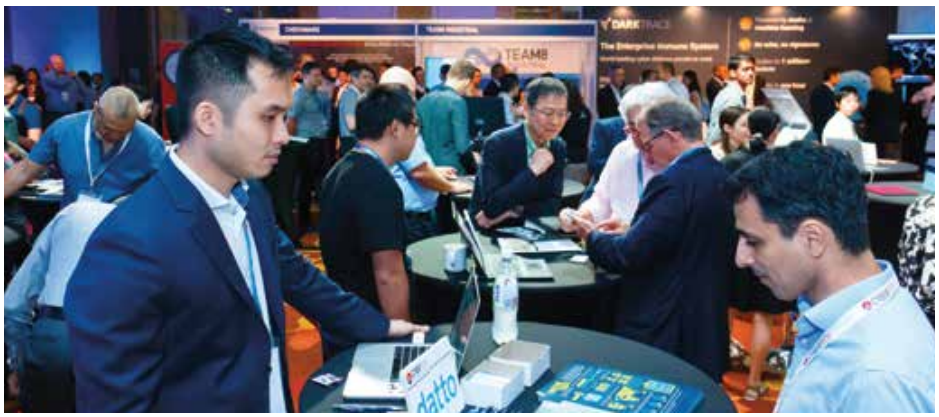
- CYBERTECH EUROPE, ROME - SEPTEMBER 26-27, 2018
- CYBERTECH MIDWEST, KICK-OFF - OCTOBER 23, 2018
- CYBERTECH TOKYO - NOVEMBER 29-30, 2018
- CYBERTECH TEL AVIV - JANUARY 28-30, 2019
- CYBERTECH LATIN AMERICA - FEBRUARY 21-22, 2019
- CYBERTECH ASIA, SINGAPORE - SPRING 2019
- CYBERTECH MIDWEST - CONFERENCE & EXHIBITION - JULY 24-25, 2019

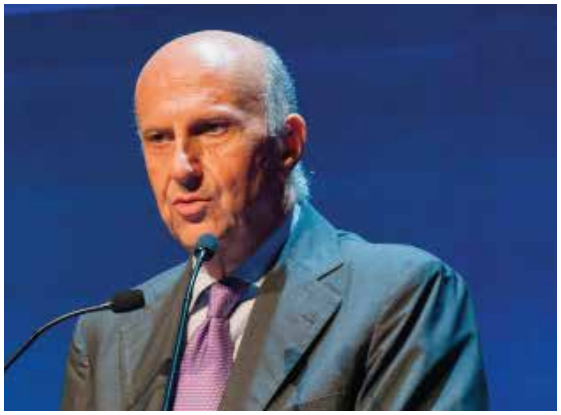
ORGANIZED BY

CYBERTECH

CYBERTECH AROUND THE WORLD

CYBERTECH TEL AVIV • **CYBERTECH** EUROPE, ROME • **CYBERTECH** SINGAPORE • **CYBERTECH** LOS ANGELES





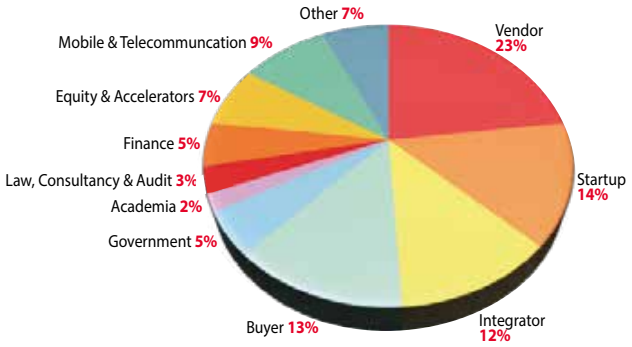
ORGANIZED BY

CYBERTECH

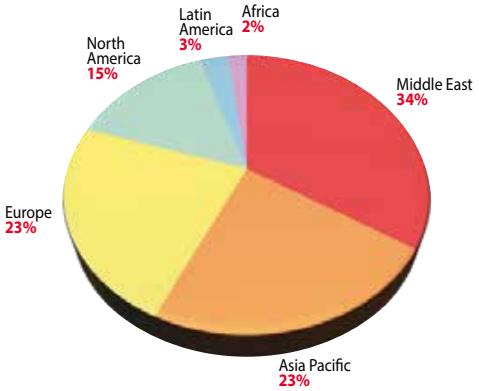
CYBERTECH TEL AVIV 2018

STATISTICS FROM CYBERTECH TEL AVIV 2018

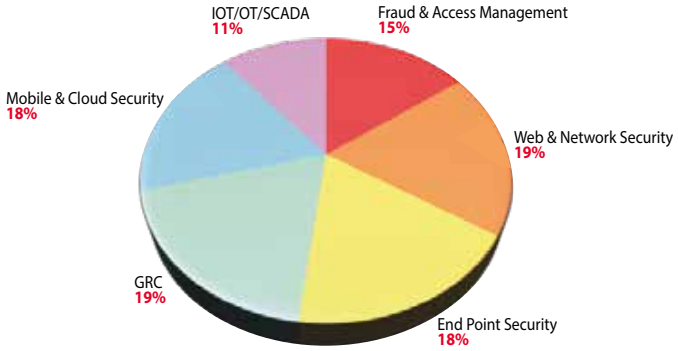
Sponsors & Exhibitors Breakdown



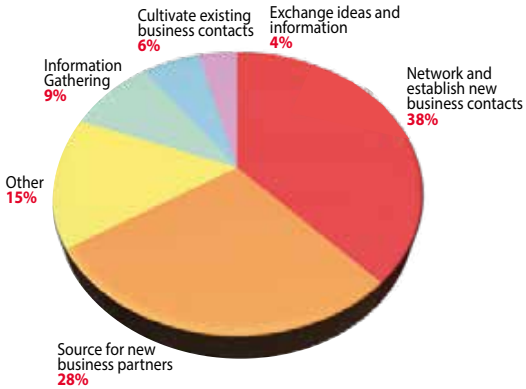
Main Market of Interest



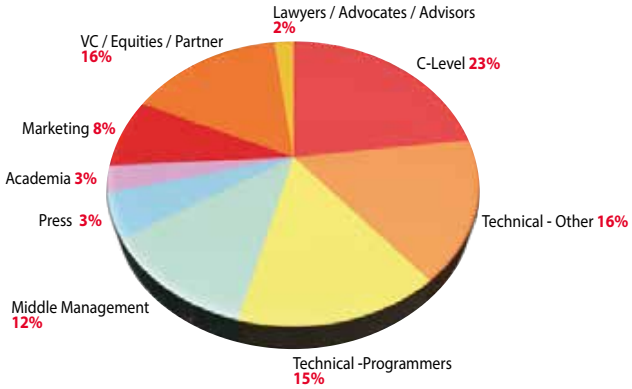
Sponsors & Exhibitors Breakdown – Cyber Security Services



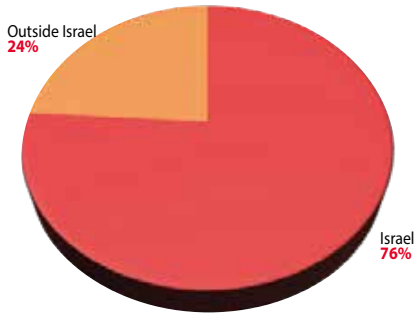
Purpose of Visit



Visitor Occupation



Country of Origin



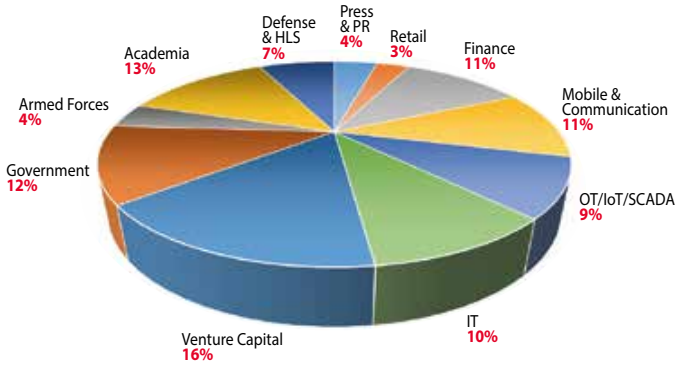
Countries with Over 80 Delegates

United States // Japan // United Kingdom // Spain // France // Italy // Germany // Singapore // Romania // Ghana // China // The Netherlands // Canada // Vietnam // Switzerland // South Korea // Brazil // India // Nigeria // Lithuania // Hong Kong // Cyprus // Poland // South Africa // Uganda // Ethiopia // Russia // Slovakia // Ukraine // Mexico // Czech Republic // Greece // Ireland

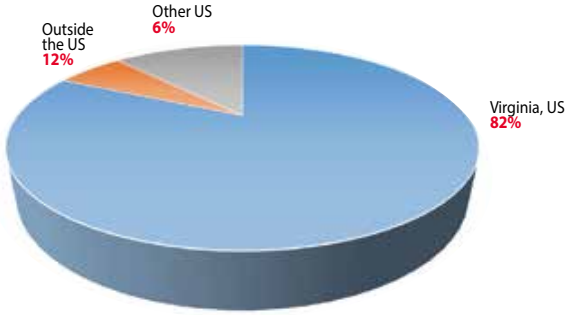
ORGANIZED BY

CYBERTECH

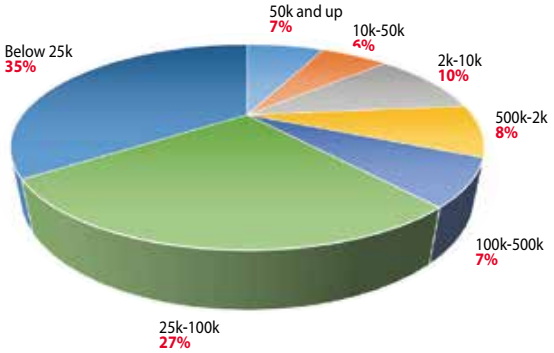
Company Classification



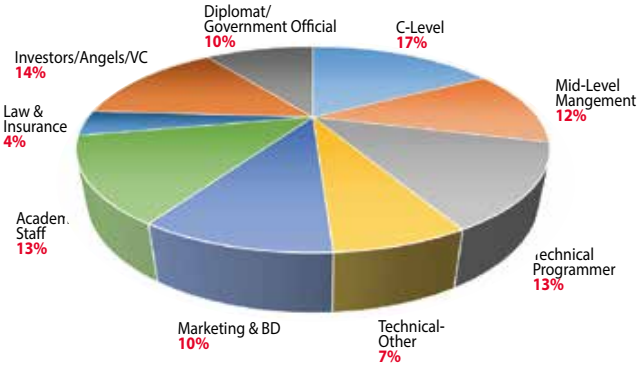
Visitor Origin



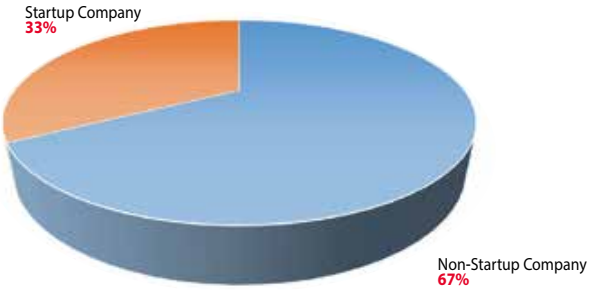
Company Size



Visitor Occupation



Startup Representation



CYBERTECH FAIRFAX 2017

FAIRFAX COUNTY
ECONOMIC DEVELOPMENT AUTHORITY

ORGANIZED BY

CYBERTECH

CYBERTECH AROUND THE WORLD

CYBERTECH EUROPE 2017 SPONSORS & EXHIBITORS

IN COLLABORATION WITH LEONARDO

INNOVATION PARTNER accenture

SPONSORS: vmware, KASPERSKY, eni, FireEye, TREND MICRO, DELL EMC, RSA, EY, FORCEPOINT, DARKTRACE, FORTINET, proofpoint, cisco, CYBERARK, McKinsey&Company, TIM, SKYBOX, CROWDSTRIKE, aizoon, enel, CITRIX, Hewlett Packard Enterprise, AVNET INTEGRATED, ITALTEL, Feedback, SELTA, NTT DATA, EXCLUSIVE NETWORKS, ForeScout, Gigamon, IMPERVA, netskope, PICUS SECURITY, CHECKMARX, CYBERSECTEAM, dgs, IAI ELTA, Deloitte., Qualys, FASTWEB, DEEPCYBER, eclectic iq, VERITAS, fis, SONICWALL, IBDO, POSITIVE TECHNOLOGIES, acea, PRISMA, Adobe, Extreme, AYARIX, VARGROUP, TAG, Avecto, IMPERVA INCAPSULA, CYBONET, Terafence, N&C, ALFA GROUP, InfoCert, EUROTECH, COBWEBS, digital shadows, ie, Hyver, PROSECS, CYS4, Cynet, SECURITY MATTERS, veeam

SPONSORS AND EXHIBITORS OF CYBERTECH WORLDWIDE EVENTS

IBM, intel, vmware, intel Security, KASPERSKY, FireEye, TREND MICRO, FORTINET, SAMSUNG, PayPal, DELL EMC, OEM, RSA, AVNET INTEGRATED, EY, FORCEPOINT, DARKTRACE, TIM, proofpoint, cisco, CYBERARK, CROWDSTRIKE, aizoon, enel, CITRIX, Hewlett Packard Enterprise, SKYBOX, Feedback, NTT DATA, EXCLUSIVE NETWORKS, CYBERSECTEAM, SELTA, Deloitte., ITALTEL, pwc, Symantec., MICRO FOCUS, Check Point, CYBERBIT, NYCEDC, IAI, intuit, RAFAEL, KENNA Security, WEBROOT, IBDO, secoz, JVP, ONTARIO CANADA, TEAM8, OPSWAT, NYOTRON, pitango, CHECKMARX, digital shadows, BAE SYSTEMS, athena dynamics, S2T, ANOMALI, Pacific Tech, CORNING Quick, PICUS SECURITY, SEPIO, merkdoo, cyber OSSERVER, endace, cybiller, SENACYT, grupovision, SYTECOM, Copa Airlines, SEC, wombat, hauzd, QUANN, Custodio, ECI, DESAY SV, Reblaze, JETRO, TDK, muRata, NEC, SBI, YASKAWA, DNP, zebra, ELRON, alcide.io, IRONSCALES, SECDO, SecuredTouch, SIXGILL, Deutsche Telekom, acea, CYS4, Akamai, InfoCert, SONICWALL, Adobe, ForeScout, INCLUDE, ALFA GROUP, Israel Electric, fis, PRISMA, FINNEGAN, VERINT, IMI SYSTEMS, Cable Onde, CTI, AT&T FOUNDRY, DEMISTO, citi VENTURES, Qualys, HYSOLATE, netskope, innov8, ZIMPERIUM, (ISC), See, 2B SECURE matrix, citi VENTURES, Gigamon, START-UP NATION CENTRAL, PROSECS, N&C, LogRhythm, algosec, TERAMIND, COMSEC Group, tufin, VERITAS, wallSSL, SenseCy, POSITIVE TECHNOLOGIES, ISARA, MER Group, IMPERVA INCAPSULA, CYBONET, GlobalSign, eclectic iq, CYGOV, Safritel, Indiana, MINERVA, GuardiCore, APERIO, ITrust, LATHAM, LIGHTCYBER, odi, CyberX, ADALLOM, cavirin, TRAPX, WATERFALL, KELA, EMET, NEXTNINE, GAV-YAM Nagev, waratek, Indegy, evolution, Safritel Canada, SentinelOne, BakerHostetler, FIRMITAS, KERNELIOS, AVNET, VARONIS, Metapacket, infosecurity EUROPE, Extreme, dgs, FASTWEB, IMPERVA, CRONUS, CYBEN, Double Rock, AllOt, VERINT, FOALIM-TECH, Team, BLUE COAT, Fasoo, amdocs, ixia, MORANGI, UNIVERSITY OF WATERLOO, APPLAUSE, Tutoroz, Bitdefender, Metapacket, HighSecLabs, KINDITE, Cynerio, ENSILO, Glilot, THETARAY, TOWERSEC, ARGUS, Avecto, innovate, radiflow, INFOBAY, SAFE-T, NATION, cryptomage, CYBERHAT, REdDOT, vertex, ERICOM, wip, wirex, FAIRFAX COUNTY, SOPHTIX, octasic, CONSIST, Experis Cyber, webhose.io, NUBO, InfoBay, SuperCom, COBWEBS, SIMPLIFY, NetFlowAuditor, CYBERJOBS, GATESCANNER, IVC Research Center, Cyberint, CloudLock, EASTRONICS, WhiteSource, Fox Rothschild LLP, INKOD, ScaleL, WIBU SYSTEMS, BALABIT, Komodo CONSULTING, CYMULATE, cybereason, vertex, 東陽テクニカ, HITACHI Inspire the Next, TMI総合法律事務所, VAULTO, SYNOPSYS, Vanmetro, verio, AYARIX, Sasa Software, cognigo, SECURITY MATTERS, Hyver, veeam, Reblaze, BigID, INTEZER, Indegy, IRI, mimecast, ie, Cynet, EUROTECH, VARGROUP, Terafence, TAG, BALABIT

ORGANIZED BY

CYBERTECH

APPENDIX D.14

EMERGENCY SERVICES & EXERCISE WORKING GROUP

EMERGENCY SERVICES AND EXERCISE WORKING GROUP STRATEGIC PLAN

Chair: Executive Director Bryan Langley | Co-Chair: Carlos Garcia

September 2018
Indiana Executive Council on Cybersecurity

Emergency Services and Exercise Working Group Plan

Contents

Committee Members **4**

Introduction **6**

Executive Summary **8**

Research **11**

Deliverable: Annex **18**

General information 18

Implementation Plan 19

Evaluation Methodology 23

Deliverable: IDHS Exercise Engagement **25**

General information 25

Implementation Plan 26

Evaluation Methodology 31

Deliverable: EOC **33**

General information 33

Implementation Plan 34

Evaluation Methodology 38

Deliverable: Toolkit **40**

General information 40

Implementation Plan 41

Evaluation Methodology 46

Supporting Documentation **49**

Indiana Department of Homeland Security (IDHS) Advancing Cybersecurity Initiatives for the State of Indiana: A Strategic Roadmap 50

Indiana Department of Homeland Security (IDHS) Crit-Ex 16.1 58

Indiana Department of Homeland Security (IDHS) Crit-Ex 16.2 90

National Governors Association (NGA) Workshop Cyber Toolkit Materials 132

Committee Members

Committee Members

Name	Organization	Title	Committee/ Workgroup Position	IECC Membership Type
Bryan Langley	IDHS	Executive Director	Chair	Voting
Carlos Garcia	IU - Emergency Management	University Director	Co-Chair	Advisory
Joe Romero	IU Health	Manager	Co-Chair Proxy	Advisory
Tom Vanderpool	Indiana Department of Transportation	Emergency Planning & Response Director	Full Time	Advisory
David Vice	Integrated Public Safety Commission	Executive Director	Full Time	Advisory
Kathy Dayhoff-Dwyer	Indiana Department of Homeland Security	Local Support Branch Director	Full Time	Advisory
Steve Berube	Citizens Energy Group	Manager of Water System Control and Planning	Full Time	Advisory
Doug Brock	American Water	Vice President of Operations	Full Time	Advisory
Cliff Campbell	Campbell Consulting	President	As Needed	Advisory
Ed Reuter	Indiana Statewide 911 Board	Executive Director	Full Time	Advisory
Debbie Fletcher	Indiana Department of Homeland Security	Exercise Training Officer	As Needed	Advisory
Erin Rowe	Indiana Department of Homeland Security	Director, Response and Recovery	As Needed	Advisory
Mike Alley	Resilient Strategies, LLC	President	Full Time	Advisory
Joe Meluch	Indiana Department of Homeland Security	Emergency Operations Center Shift Manager	Full Time	Advisory
Jonathon Barefoot	Ivy Tech Community College	Executive Director of Statewide Safety and Security	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - **National Incident Management System (NIMS)**: A comprehensive, national approach to incident management that is applicable at all jurisdictional levels and across functional disciplines.
  - **Emergency Management Accreditation Program (EMAP)**: A set of 64 professional emergency management standards designed as a tool for continuous improvement as part of a voluntary accreditation process for local, state, federal, higher education and tribal emergency management programs.
  - **National Fire Protection Association (NFPA) Standard 1600 - Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs**: A common set of criteria for all hazards disaster/emergency management and business continuity programs.
  - **Centers for Medicare and Medicaid Services (CMS) Emergency Preparedness Rule:** Establishes national emergency preparedness requirements for healthcare entities to ensure adequate planning for both natural and man-made disasters, and coordination with federal, state, tribal, regional and local emergency preparedness systems.
  - **The Joint Commission Emergency Management Standard:** Healthcare accreditation standards outlining program requirements for preparedness, mitigation, response, and recovery phases of emergency management.
  - **Presidential Policy Directive (PPD) 41 – U.S. Cyber Incident Coordination:** This directive sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities**.**
  - **Health Insurance Portability and Accountability Act (HIPAA) Security Rule:** Federal information security requirements put in place to safeguard individuals' electronic protected health information.
  - **Homeland Security Exercise Evaluation Program (HSEEP):** Provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.
  - **United States Computer Emergency Readiness Team (US-CERT):** Organizations within the U.S. Department of Homeland Security tasked with providing cyber incident prevention, protection, preparedness, response, and recovery capabilities to federal, state, local, and tribal government agencies.

- **Research Findings**
  - Existing national standards and best practices for emergency preparedness and all-hazard incident management are applicable to cybersecurity initiatives.
  - The basic concepts for emergency planning, training, exercise, evaluation, and improvement can be implemented as the foundation for cybersecurity preparedness programs.
  - An abundance of cybersecurity information and services are available to individuals, government agencies, and private sector organizations.

- There is, however, a lack of affordable, easily accessible tools and resources geared specifically for small business and small local government entities.
- There no central point of coordination and information sharing for state-level cybersecurity planning, training, and exercise activity.

- **Working Group Deliverables**
  - Conduct review of the Cyber Annex to State of Indiana Comprehensive Emergency Management Plan.
  - Draft recommendations for revisions to the Cyber Annex and development of a coordinating entity within the Indiana State Emergency Operations Center.
  - Develop threat assessment, planning, training, and exercise toolkit for local government and small businesses.
  - Create guidance for coordination of local government, private sector, and state government cybersecurity drill and exercise activity.

- **Additional Notes**
  - No additional information at this time.

- **References**
  - **National Incident Management System (NIMS)**: https://www.fema.gov/national-incident-management-system
  - **Emergency Management Accreditation Program (EMAP)**: https://www.emap.org/
  - **National Fire Protection Association (NFPA) Standard 1600:** https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600
  - **Centers for Medicare and Medicaid Services (CMS) Emergency Preparedness Rule:** https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule.html
  - **The Joint Commission Emergency Management Standard:** https://www.jointcommission.org/emergency_management.aspx
  - **PPD 41 – U.S. Cyber Incident Coordination:** https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
  - **Homeland Security Exercise Evaluation Program (HSEEP):** https://www.fema.gov/hseep
  - **Health Insurance Portability and Accountability Act (HIPAA) Security Rule:** https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
  - **U.S. Computer Emergency Readiness Team (US-CERT):** https://www.us-cert.gov/

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    - **COMPLETED ACTIONS**
        - 2015 State Cybersecurity Reference Guide – Drawing from the 2009 Cybersecurity Strategy, this document provides an overview of national best practices, professional standards, and provides case studies of cybersecurity programs in other states.
        - Supervisory Control and Data Acquisition (SCADA) Smartbook is completed, outlining Industrial Control System risks to critical infrastructure.
        - Management and oversight of joint public/private/military cybersecurity exercises have been transferred from the Indiana Chapter of Infragard to Indiana Department of Homeland Security (IDHS).
        - IDHS completes State Strategic Roadmap to Cybersecurity, outlining five essential pillars.
        - Crit-Ex 16.1 Cyber Disruption Tabletop Exercise is completed. Government, emergency management, water utilities, and power utilities discuss responding to a long-term regional power outage.
        - Crit-Ex 16.2 Functional Exercise is completed. Water utilities respond to a cyberattack on a water treatment facility's SCADA system at Muscatatuck Urban Training Center (MUTC).
        - Governor's Council on Cybersecurity is established via EO and launched.
        - Crit-Ex Cybersecurity Awareness Seminar is completed – first in a series of progressively sophisticated exercises for 2016-2017.
        - Significant Cyber Incident Response Annex to State CEMP Workshop is held.
        - IDHS Training & Exercise completes Cybersecurity Awareness Seminars for Emergency Management Administrators (EMAs) in districts 5, 6, and 7.
        - Continuity/Cybersecurity workshops are brought into local jurisdictions, designed by Federal Emergency Management Agency (FEMA) and US DHS.
    - **CURRENT ACTIONS**
        - Draft version of Significant Cyber Incident Response Annex is under review.
        - Identification and outreach with subject-matter experts, policymakers, and executive leadership for inclusion in the State's cybersecurity program governing and project management bodies.
        - Inventory and support cyber grant opportunities for local and CI partners.
    - There have been a number of exercises and trainings across the state that touch on cybersecurity and directly correspond public safety and emergency services. Examples of these include:
        - Indiana Office of Technology – Cyber Security Mentoring Program

        - State of Indiana Joint Full-Scale Exercises – CritEx – 2015 and 2016 (Electrical Grid response) at Muscatatuck Urban Training Center
        - Cyber Security-Based Tabletop Exercises – Private Sector, International Manufacturing, Higher Education
        - Hamilton County (Indiana) Threat and Hazard Identification and Risk Assessment Exercise focusing on Cyber Response – 2017
        - Ivy Tech has bi-annual training on Cyber Security for staff and adjunct faculty

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    - Critical infrastructures and emergency service sectors
    - In a conference call in December 2017 to discuss these questions, the Working Group proposed that the primary vulnerabilities in each of our areas fall generally in the following three (3) areas:
        - People – human error, lack of training, or actual intent to cause harm are all people-oriented vulnerabilities that can be mitigated or reduced.
        - Process – Key procedures, protocols, and policies related to the need to lessen or prevent cyber incidents has to be in place and directed toward all areas of vulnerabilities within a given agency, department, and/or sector.
        - Technology – new or emerging technologies to lessen or prevent vulnerabilities also seem to prompt hackers/criminals to test or challenge new systems, software, hardware, etc.

3. **What is your area's greatest cybersecurity need and/or gap?**
    - Resources to serve all those in need for the state is a significant need.
    - In a meeting and conference call conducted on December 2017 to discuss these questions, the Working Group all agreed the most significant cybersecurity need or gap continues to be the following:
        - Frequent and on-going training frontline system users and staff
        - Engaged and targeted outreach programs for all users and staff covering various areas of cyber incidents
        - Technical planning and process review
        - IT/Cyber Security cross training and engagement

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    - **National Incident Management System (NIMS)**: A comprehensive, national approach to incident management that is applicable at all jurisdictional levels and across functional disciplines.
    - **Emergency Management Accreditation Program (EMAP)**: A set of 64 professional emergency management standards designed as a tool for continuous improvement as part of a voluntary accreditation process for local, state, federal, higher education and tribal emergency management programs.
    - **National Fire Protection Association (NFPA) Standard 1600 - Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs**: A common set of criteria for all hazards disaster/emergency management and business continuity programs.

- **Centers for Medicare and Medicaid Services (CMS) Emergency Preparedness Rule:** Establishes national emergency preparedness requirements for healthcare entities to ensure adequate planning for both natural and man-made disasters, and coordination with federal, state, tribal, regional and local emergency preparedness systems.
- **The Joint Commission Emergency Management Standard:** Healthcare accreditation standards outlining program requirements for preparedness, mitigation, response, and recovery phases of emergency management.
- **Presidential Policy Directive (PPD) 41 – U.S. Cyber Incident Coordination:** This directive sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities**.**
- **Health Insurance Portability and Accountability Act (HIPAA) Security Rule:** Federal information security requirements put in place to safeguard individuals' electronic protected health information.
- **Homeland Security Exercise Evaluation Program (HSEEP):** Provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.
- **United States Computer Emergency Readiness Team (US-CERT):** Organizations within the U.S. Department of Homeland Security tasked with providing cyber incident prevention, protection, preparedness, response, and recovery capabilities to federal, state, local, and tribal government agencies.
- **State Law Title 10**
- In a meeting and conference call conducted on December 12, 2017 to discuss these questions, the Work Group did not provide a list of federal, state or local cyber regulations, but instead, asked that the following authorities, as listed in the State of Indiana's Cyber Emergency Response Annex, be reviewed for accuracy and completeness:
    - **Federal**
        - The National Cyber Incident Response Plan (NCIRP)
        - National Response Framework (NRF)
        - The National Incident Management System (NIMS) Homeland Security Act of 2002
        - Homeland Security Presidential Directive
        - Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended. 42 United States Code 5121, et seq.
        - Code of Federal Regulations. Title 44, Part 205 and 205.16.
        - Buckle, Philip. (1999). "Re-defining Community and Vulnerability in the Context of Emergency Management." Australian Journal of Emergency Management (Summer): 21-26.
        - Guidance on the National Incident Management System (March 2008)
        - Guidance on the National Preparedness Goal (September 2007)
        - National Strategy to Secure Cyberspace, February 2003
        - National Cyber Incident Response Plan, Interim Version, September 2010

        - Cyber Incident Annex, National Response Plan, December 2004
        - Strengthening Regional Resilience through National, Regional, and Sector Partnerships, National Infrastructure Advisory Council (2013)
        - DoD Strategy for Operating in Cyberspace (DSOC), July 2011
        - Cyber Security Framework Strategy For the State of Indiana, 2009
    - **State**
        - Indiana Code 10-14-3, Emergency Management and Disaster Law
        - A Leader's Guide to Emergencies and Disasters, IDHS (September 2008)
        - Executive Order 13-09, January 2013
    - **Local**
        - County/Local Emergency Management Ordinances

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    - 12 DHS CI Sector Specific Plans
    - Memo and report of benchmark research of other state response plans
    - 19 specific State Incident Response Plans/strategies
    - Indiana Crit-Ex reference documents and reports
    - Indiana Comprehensive Emergency Management Plan
    - Personnel present and those who called into the meeting were asked to provide information or previous cyber incidents or case studies to be included with this report.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    - Other State Incident Plans
    - National Governors Association State Studies
    - IDHS Advancing Cybersecurity Initiatives for the State of Indiana Roadmap
    - Preparedness Cycle Implementation Presentation – Indiana
    - IDHS Cyber SmartBook
    - Personnel present and those who called into the meeting were asked to provide information or previous incident to support the group's deliverables.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    - See references for other state cyber plans and incident plans.
    - See above – Item #1

8. **What does success look like for your area in one year, three years, and five years?**
    - Conduct review of the Cyber Annex to State of Indiana Comprehensive Emergency Management Plan.
    - Draft recommendations for revisions to the Cyber Annex and development of a coordinating entity within the Indiana State Emergency Operations Center.

- Develop threat assessment, planning, training, and exercise document templates for local government and small businesses.
- Create guidance for coordination of local government, private sector, and state government cybersecurity drill and exercise activity.
- Develop "tabletop toolkits" with IDHS exercise support, including a cyber TTX, for local partners.
- Exercise Cyber Incident Response Annex to identify gaps.
- Develop the Statewide Cybersecurity Strategic Plan within the Cybersecurity Council.
- Determine future Crit-Ex direction.
- In a meeting and conference call conducted on December 2017 to discuss these questions, the Work Group described success over the short- and long-term as having the following factors:
    - Significant reduction or elimination of cyber incident in all critical sectors within the State of Indiana
    - The ability to effectively target and protect against new and emerging cyber threats
    - Make cyber response exercises a continual and frequent tool to validate and show improvement in the state's overall capability to meet cyber threats head on

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    - An abundance of cybersecurity information and services are available to individuals, government agencies, and private sector organizations.
    - There is no central point of coordination and information sharing for state-level cybersecurity planning, training, and exercise activity.
    - In a meeting and conference call conducted in December 2017 to discuss these questions, the Work Group provided the following as key in promoting public awareness and understanding of cyber incidents:
        - Having cybersecurity messaging and outreach directed toward the general public, similar to the US Department of Homeland Security's "See Something, Say Something" program
        - General and frequent Public Service Announcements (PSAs) targeting specific sectors and portions of the populations, providing tips and considerations for lessening or eliminating cyber threats and incidents
        - Developing and targeting education and cybersecurity training for public safety warning points and dispatch centers as a means to meeting the needs of first responders

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    - Workforce in this area is focused on training emergency managers, departments, etc.
    - No clear answers given for this question from the group – Each member was asked to provide their answers individually.

11. **What do we need to do to attract cyber companies to Indiana?**
    - In a meeting and conference call conducted on December 2017 to discuss these questions, the Work Group provided the following items to address how we can attract cyber companies to Indiana:
        - Involve Workforce Development in targeting and highlighting jobs in the field, while also offering training and job skill support
        - Working with private and public universities and colleges within the state to expand and enhance degree programs to target cyber processes, threat reduction, and innovation

12. **What are your communication protocols in a cyber emergency?**
    - Indiana is in the process of finalizing it state Cyber Annex.
    - Personnel present and those who called into the meeting were asked provide information on their organization's communications protocols for a cyber emergency.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    - Existing national standards and best practices for emergency preparedness and all-hazard incident management are applicable to cybersecurity initiatives.
    - The basic concepts for emergency planning, training, exercise, evaluation, and improvement can be implemented as the foundation for cybersecurity preparedness programs.
    - Personnel present and those who called into the meeting were asked to provide information on best practices for their specific sector to identify, lessen or eliminate cyber threats and incidents.

Deliverable: Annex

Deliverable: Annex

General information

1. **What is the deliverable?**
   a. Finalize IDHS Cyber Annex to CEMP

2. **What is the status of this deliverable**?
   a. In-progress; 75% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See [Executive Order 17-11] for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Complete the IDHS Cyber Annex

6. **What metric or measurement will be used to define success?**
   a. Annex to be completed and finalized with all the parties who are required to sign off on it per IDHS CEMP internal requirements.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Emergency response agencies and partners

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. This is an annex to the State of Indiana's CEMP produced and executed by IDHS during declared emergencies.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Government Services Committee

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IDHS, Indiana State Police (ISP), Indiana National Guard (INNG), Indiana Office of Technology (IOT), 911 Board, and Governor's office.

12. **Who should be main lead of this deliverable?**
    a. IDHS

13. **What are the expected challenges to completing this deliverable?**
    a. Ensuring that once finalized that the annex is exercised appropriately before an emergency occurs.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review Annex from IDHS – Preliminary review with key stakeholders	Cybersecurity Program Director/IDHS/IOT/ISP/INNG	100%	2017	
Rewrite Annex	Cybersecurity Program Director and Emergency Services and Exercise Working Group leads	100%	July 2018	
Working Group Review	Emergency Services and Exercise Working Group	100%	September 2018	
Committee Review	Government Services Committee	0	October 2018	
Finalize Annex	IDHS	0	November 2018	
Distribute/Communicate Annex to key stakeholders	IDHS	0	December 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Greatest benefit is to provide an operational framework that can guide response activity across multiple agencies, government, and private organizations.

18. **How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?**
    a. By a coordinated effort, the annex will allow private, public, and government organizations to respond to cyber emergencies efficiently and effect in a more coordinated fashion; therefore, reducing the potential for cybersecurity risk or possible impact.

19. **What is the risk or cost of not completing this deliverable?**
    a. The lack of coordination and possible mass confusion during a cyber emergency can increase the cybersecurity risk and negative impact on affected critical infrastructures and Indiana.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Completion of annex and testing that it is an operational plan.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. The National Governor's Association and FEMA identified several other states who have a cyber annex.
22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. The National Governor's Association and FEMA identified several other states who do not have a cyber annex.

Other Implementation Factors

---

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. Approval and consensus of all the functions of Indiana's CEMP Cyber Annex may be difficult among key stakeholders.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. To review the Annex every 2-3 years and after a real-world incident.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. N/A

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All critical infrastructure sectors

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Appropriate contacts within the critical infrastructure sectors, key emergency management stakeholders, key state agencies executives, Governor's office, enforcement agencies.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No

30. What are other public relations and/or marketing considerations to be noted?

a. The CEMP's Cyber Annex is meant to be an internal document and shared with those who are a "need to know" basis only.

Evaluation Methodology

Objective 1: IDHS will develop and distribute the IDHS CEMP Cyber Annex to appropriate parties by December 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IDHS will exercise the IDHS CEMP Cyber Annex by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: IDHS Exercise Engagement

Deliverable: IDHS Exercise Engagement

General information

1. **What is the deliverable?**
   a. IDHS Cyber Exercise Engagement Program

2. **What is the status of this deliverable?**
   a. Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☒ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. IDHS Cyber Exercise Engagement Program to be used by public, private, military, and government sectors so that state response can be realistically incorporated into cyber exercises being conducted throughout the State of Indiana.

6. **What metric or measurement will be used to define success?**
   a. Stakeholders are made aware of the completed program and use it.

7. **What year will the deliverable be completed?**
   a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Public, private, military, and government sectors

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None at this time.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None at this time.

12. **Who should be main lead of this deliverable?**
    a. IDHS

13. **What are the expected challenges to completing this deliverable?**
    a. Completing with current IDHS resources and communicating the new program to stakeholders who would benefit. Once stakeholders begin using program there may be limitations on how much exercising IDHS can participate in.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort – it will need to continue to be updated and

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review and Finalize Cyber Annex	Cybersecurity Program Director/IDHS/IOT/ISP/INNG	100%	2018	
Create internal Cyber Exercise Engagement Program Planning team	IDHS	0	March 2019	
Create Cyber Exercise Engagement Program	IDHS	0	July 2019	
Develop Cyber exercise based on annex and risk profile	IDHS	0	Fall 2019	
Conduct Cyber exercise based on annex and risk profile	IDHS	0	December 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
One FTE	One FTE	EM with cyber-focused planning background	EMPG/SHSP Grant funding		Already exists in IDHS budget. Other IDHS staff assist in creating the workshops, toolkit support, and sustainability

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Printing cost	Cyber Workshops	$1000.00	TBD	EMPG		2019 Proposal needed
Travel Costs	Cyber Workshops		TBD	EMPG		

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The Exercise Engagement Group will allow government entities, businesses, and related nonprofits to partner together and exercise to a more unified and cost-effective response to a cyber incident, improving all preparedness capabilities.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Governments (state and local level), small businesses and other partners will be more prepared for a cyber incident response will reduce the cybersecurity risks to the State of Indiana and possible impacts during a cyber emergency.

19. What is the risk or cost of not completing this deliverable?

a. No cost. Rather, not having a reviewed, trained, and exercised a cyber incident response plan can have a high impact not only on the effective response capability of the State of Indiana but can cause longer than expected disruption to the business or local government.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion of deliverable and meeting key milestones will be one measure of success. Timeline, scope of delivery, and quality of product are key measures.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes – at varying levels. Requires more research and decision-making by working group.
b. **If Yes, please list states/jurisdictions**
    i. [No Response]

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The timeline and completion of the cyber annex drives the next steps in the planning, training, and exercise process. In addition, staff, monetary resources, or administrative priorities could change or slow the timeline of the project down.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. Perhaps a change in internal (IDHS) project/policy priorities but no regulation or statutory changes.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. A review and update of the exercise based on feedback and emerging threats and technology will need to be considered regularly due to changes in the risk profile and ever-changing cyber culture. Additionally, workshops and training should be improved upon, further developed, and made available throughout the state to increase its use and effectiveness.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. IDHS Executive Director Bryan Langley

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. Public (all levels, mostly local), private, nonprofit, other nongovernmental

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. IECC members, local government, business associations, emergency management professionals, state and federal partners.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. TBD at a later date.

Evaluation Methodology

Objective 1: IDHS will develop and launch Cyber Exercise Engagement Program by July 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Emergency Operations Center (EOC)

Deliverable: EOC

General information

1. **What is the deliverable?**
    a. Indiana State Emergency Operations Center Cyber Coordination procedures and implement the process of how the state responds to a cyber emergency, with guidance from the Cyber Emergency Response Annex to the Comprehensive Emergency Management Plan.

2. **What is the status of this deliverable?**
    a. In-progress; 25% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☒ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Develop a coordinating entity within the Indiana State Emergency Operations Center

6. **What metric or measurement will be used to define success?**
    a. Complete the product

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Emergency management partners, sector partners, government partners

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Government Services

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IDHS, ISP, IOT, INNG, IECC

12. **Who should be main lead of this deliverable?**
    a. IDHS

13. **What are the expected challenges to completing this deliverable?**
    a. Ensuring that all those who would benefit from using this EOC coordinating procedure is aware of it and making sure it is exercised appropriately before an emergency occurs.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Create/Update Org Charts	State EOC		CERA completion + 30 days	
Create SOPs	State EOC		CERA completion + 30 days	
Create duty descriptions	State EOC		CERA completion + 30 days	
Identify Players	Chetrice Mosely/Director Langley		CERA Completion +30 days	
Conduct training	State EOC		CERA completion + 60 days	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A – no additional IDHS staff; perhaps additional physical seat or workspace		EOC Training/ leverage existing skills			

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None

Resource	Justification/ Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Formalized organization and training of personnel in anticipation of a cyber emergency.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Impact could be reduced by having a prepared, coordinated response. There will be mutual understanding between responders, which will increase efficiency.

19. What is the risk or cost of not completing this deliverable?

a. Risking uncoordinated response, delayed acquisition of resources, general lack of understanding during an incident.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success will be defined by the effectiveness of a response. Because of the difficulty in quantifying success, qualitative data must be utilized, primarily through opinions derived by after action reports. These reports will indicate what portions of a response went well and what did not.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. Michigan, Arizona, Maryland

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. There are certainly some jurisdictions that lack a formal cyber incident response plan, but determining the consequence of no plan may prove difficult

Other Implementation Plan

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The timeline and Completion of the cyber annex drives the next steps in the planning, training, and exercise process. In addition, staff, monetary resources, or administrative priorities could change or slow the timeline of the project down.
b. Lack of support for the CERA may delay delivery.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. A review and update of the exercise based on feedback and emerging threats and technology will need to be considered regularly due to changes in the risk profile and ever-changing cyber culture. Additionally, workshops and training should be improved upon, further developed, and made available throughout the state to increase its use and effectiveness.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. IOT, ISP, and INNG have been partners in the development of the CERA.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. Any sector; using the documents as templates and guidance for organizing a response to a cyber incident. This can guide other sectors as to who is responsible for what within state government, and each sector can adjust their plans accordingly.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Any stakeholder with responsibility outlined in the plan.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No

30. What are other public relations and/or marketing considerations to be noted?

a. TBD at a later date.

Evaluation Methodology

Objective 1: IDHS will develop a Cyber Liaison position within Emergency Operations Center by May 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IDHS will complete training and exercise the Cyber Liaison position within the EOC by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Toolkit

Deliverable: Toolkit

General information

1. **What is the deliverable?**
    a. Develop a Cyber Incident Planning and Preparedness Toolkit for Emergency Managers that is compliant with FEMA, USDHS, and NIST. *See NGA Policy Academy Notes for further details.*

2. **What is the status of this deliverable?**
    a. In-progress; 50% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☒ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☒ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Emergency Managers treat each cyber incident like any other hazard. Assist stakeholders with developing, planning, and preparing for a cyber incident.

6. **What metric or measurement will be used to define success?**
    a. Completion of the toolkit and providing it to stakeholders

7. **What year will the deliverable be completed?**
    a. Version 1 – 2018
    b. Version 2 – 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Stakeholders include local government, small businesses, and state agencies

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State preparedness report, federal grant programs, and Hazard Identification and Risk Assessment (HIRA). More information about the HIRA can be found at https://www.in.gov/dhs/3879.htm.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Not currently.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IECC working groups and partners

12. **Who should be main lead of this deliverable?**
    a. IECC Emergency Services and Training Working Group to develop
    b. State of Indiana to promote
    c. IDHS to provide support and subject matter expertise in assisting with training and exercising among local government/EMAs

13. **What are the expected challenges to completing this deliverable?**
    a. Ensuring that those who want to use the toolkit can receive assistance, guidance, and training in using the toolkit.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Gather current resources and templates for incident response toolkit	Joe Romero	100%	June 2018	
Create toolkit – version 1	Joe Romero and Carlos Garcia	75%	October 2018	
Develop cyber workshops	IDHS	0	January - August 2019	
Conduct cyber workshops	IDHS	0	October 2019	
Develop cyber risk profile tool and toolkit 2.0	Joe Romero, Carlos Garcia, Cybersecurity Program Director	15%	August 2019	National Governors Association Project (see supporting documentation)
Develop cyber incident workshops plan	IDHS	0	August – December 2019	
Conduct Cyber incident workshops	IDHS	0	March 2020	
Make improvements to toolkit	IDHS	0	August 2020	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0.5 FTE	0.5 FTE	Emergency Management	State of Indiana	N/A	IDHS to assist in creating the workshops, toolkit support, and sustainability

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. The toolkit will provide a user template planning documents geared towards small businesses and local government entities that may not have the financial resources or personnel to develop complex response plans and training programs.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Small businesses and local governments being more prepared for a cyber incident response will reduce the cybersecurity risks to the State of Indiana and possible impacts during a cyber emergency.

19. What is the risk or cost of not completing this deliverable?

a. Not having a cyber incident response plan due to lack of financial resources or personnel can have a high impact not only on the effective response capability of the State of Indiana but can cause longer than expected disruption to the business or local government.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion of deliverable and meeting key milestones will be one measure of success. End-user success in effectively using the toolkit will be an additional measure of success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. Small Business Administration, Federal Communications Commission (FCC), and FEMA have templates to use in incident response planning.

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. While there are planning resources from ISACs and FEMA, there are not any comprehensive planning toolkits created by other states to this degree that could be found geared to small businesses and local government that does not have a high knowledge in information technology and emergency management.

Other Implementation Factors

---

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. The risk profile tool may not be complete due to resources by the first year, but can certainly be completed in year two of the IECC.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. A review of the toolkit based on feedback and emerging threats and technology will need to be considered annually. Additionally, workshops and training should be made available throughout the state to increase its use and effectiveness.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. Have contacted Purdue regarding risk assessments and IU Health Chief Information Security Officer (CISO) regarding specific cyber risks.

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. All

Communications

---

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. IECC members, local government, business associations, emergency management professionals, state and federal partners

29. **Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?**
    a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC Emergency Services and Exercise Working Group will develop a Cyber Response Toolkit 1.0 by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IDHS will launch four workshops throughout Indiana using the Cyber Response Toolkit by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 3: Partnering with the National Governors Association, the IECC Emergency Services and Exercise Working Group will develop a Cyber Response Toolkit 2.0 with a cyber risk tool for emergency personnel by August 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 4: IDHS will develop and launch four workshops throughout Indiana using the Cyber Response Toolkit 2.0 by March 2020.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- 2015 Advancing Cybersecurity Initiatives for the State of Indiana: A Strategic Roadmap
- Crit-Ex 16.1
- Crit-Ex 16.2
- National Governors Association – Workshop Cyber Toolkit Materials – August 2018

Indiana Department of Homeland Security (IDHS)

Advancing Cybersecurity Initiatives for the State of Indiana: A Strategic Roadmap

April 2018

Indiana Department of Homeland Security

Advancing Cybersecurity Initiatives for the State of Indiana: A Strategic Roadmap

PURPOSE

This document establishes a common operating picture of previous and current public and private sector cybersecurity activity and serves as a roadmap for establishing a comprehensive cybersecurity strategy for the State of Indiana.

MISSION

Desired Cybersecurity Outcomes as Established by the Office of the Governor:

1. Develop and implement a state cybersecurity strategy.
2. Maintain a preparedness-based protective posture.
3. Pursue and enhance statewide cyber incident response capabilities.

BACKGROUND

Numerous, high-profile incidents involving security breaches and data theft from government agencies and large corporations illustrate the vulnerability that exists. Data breaches are, and will continue to be, a significant issue for both the public and private sector. While the theft of data and the resulting financial consequences affect government agencies, large corporations, and private citizens, a disturbing trend has begun to emerge in recent years. Industrial control systems, complex computer networks used to operate industrial production equipment and public utility infrastructure, have also come under attack in recent years.

Unlike intrusion into information technology systems, which results in the loss of data, the compromise of industrial control systems can allow attackers to take control of physical infrastructure and mechanical systems. This evolving threat puts complex manufacturing, energy infrastructure, water utilities, and petrochemical production systems at risk for attack. In 2012 alone, The U.S. Department of Homeland Security reported nearly 200 attacks on industrial control systems, 40% of which were against energy production and distribution systems.

The idea that the United States is facing a “Cyber 9/11” is at the forefront of homeland security discussion nationwide. Like the rest of the country, the State of Indiana has a short window of opportunity to prepare for a major cybersecurity incident that, if successful, could be as devastating as a major earthquake or tornado. At this time, however, the State lacks a comprehensive strategy for preventing, protecting, mitigating, responding to and recovering from cyber incidents affecting critical infrastructure, key resources, and essential services statewide.

Securing Indiana’s information technology infrastructure and industrial control systems is beyond the reach of any single entity. The diverse authorities, roles, and responsibilities of critical infrastructure stakeholders require a collaborative partnership that encourages unity of effort. The Indiana Department of Homeland Security (IDHS), Indiana Office of Technology (IOT), and the Indiana National Guard (INNG) are leading a statewide, collaborative effort involving government, private-sector, military, research, and academic stakeholders to enhance Indiana’s cybersecurity posture. It will be through this unique partnership that the State of Indiana will develop a strategic vision, consolidate and coordinate its efforts, and turn good ideas and policy into effective action.

SITUATION

Numerous local, state, and federal agencies, military and private-sector entities, universities, and research groups within the State of Indiana are actively pursuing cybersecurity initiatives. Though these individual efforts do enhance the level of cybersecurity, these improvements are often sector-specific and narrow in scope. The current threat environment requires a state-driven effort to synchronize independent cybersecurity programs into a coordinated and unified effort.

COMPLETED ACTIONS

- 2015 State Cybersecurity Reference Guide – Drawing from the 2009 Cybersecurity Strategy, this document provides an overview of national best practices, professional standards, and provides case studies of cybersecurity programs in other states.
- Comprehensive review of ISO 27000 Series standards, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, applicable Presidential Policy and Homeland Security Presidential Directives, US DHS Cybersecurity Strategy for the Homeland Security Enterprise, and the National Infrastructure Protection Plan.
- Draft Indiana National Guard Cyber Incident Response Plan completed.
- "Cyber Shield" exercises successfully conducted by the Indiana National Guard.
- State Level Exercise 2017 scheduled at the Muscatatuck Urban Training Center (MUTC). Exercise scenario will be a coordinated cyber attack on public power and water utilities.
- IOT incident response protocols for state information networks are in place, as are IT disaster recovery procedures and secure off-site data centers.
- Management and oversight of joint public/private/military cybersecurity exercises has been transferred from the Indiana Chapter of Infragard to IDHS.
- Manager hired for the Security Operations Center, the first operational element of the Indiana Information Sharing and Analysis Center (IN-ISAC).

CURRENT ACTIONS

- Comprehensive Strategy for State Cybersecurity – Initial draft under development.
- Review and migration of IOT security protocols from ISO to NIST standards.
- Restructuring and re-purposing existing executive steering committee and core project team under IDHS leadership.
- Re-branding and re-launching of "CritX" cybersecurity exercise program.
- Identification and coordination of current State agency and private-sector stakeholder cybersecurity activity.
- Identification and outreach with subject-matter experts, policy makers, and executive leadership for inclusion in the State's cybersecurity program governing and project management bodies.

FUTURE ACTIONS

-Short-Term Target Dates (3 to 6 months)

- Strategic roadmap document completed – August 1st, 2015
- Initial Draft - Preparedness framework completed – August 7th, 2015
- Initial Draft - Response protocol framework completed – August 14th, 2015
- Convene Cybersecurity Executive Steering Committee – August 2015
- Convene Cybersecurity Core Project Team – August 2015
- Initial Draft - Comprehensive Strategy for State Cybersecurity completed – September 1st, 2015
- Final Draft - Comprehensive Strategy for State Cybersecurity completed – October 1st, 2015
- Cybersecurity Awareness Month – October 2015
- IN-ISAC Promotional Launch – October 2015
- Cybersecurity Exercise Series Launch – October 2015
- Initial Draft – Cybersecurity and Information Assurance ESF Annex – December 2015

PROPOSED STRATEGIC INITIATIVES

1.0 GOVERNANCE - Establish an effective cybersecurity governance structure and strategic direction

- 1.1 State Cybersecurity Council
- 1.2 Cybersecurity Core Team
- 1.3 Project Working Groups

Maintaining an evolved cybersecurity posture requires a multi-level governance structure. A Core Team comprised of representatives from government, military and private-sector organizations will keep apprised of changes in the cyber ecosystem, ensure the continued viability of the State strategy, and designed forward-thinking programs and initiatives. It will operate at the direction of the executive-level Cybersecurity Council, which will also act as the implementing arm of policy proposed by the Core Team. Supporting working groups will manifest on an as-needed basis to supply subject-matter expertise on specific issues, such as Private-Sector Engagement, Risk Analysis, and Industrial Control Systems.

2.0 INTEGRATION – Formalize strategic cybersecurity partnerships

- 2.1. Define State, FBI, INNG, DHS, ISP, and private-sector roles and responsibilities
- 2.2. Assess & integrate capabilities
- 2.3. Align goals and objectives

Convene sector-specific representation to define individual roles for cyber emergency management and solicit ongoing input. Cybersecurity Council and Core Team membership will reflect a commitment to integration across agencies, sectors, jurisdictions, and levels of government. This approach relies on the expertise of state, local and federal government agencies; the Indiana National Guard; academic and research; critical infrastructure stakeholders; and the private sector.

3.0 PREPAREDNESS - Strengthen best practices through effective prevention, protection & mitigation

- 3.1. Establish state agency cybersecurity policies, standards, and key performance indicators
- 3.2. Establish and communicate best practices to external public and private sector stakeholders
- 3.3. Effectively coordinate and conduct planning, training, and exercise activity

A key strength of the State's cybersecurity strategy will be the best practices and tools it offers to stakeholders in order to yield a more robust preparedness posture. IOT has defined key performance indicators for departments in the State Executive branch using NIST and ISO27000. IDHS will use these metrics to draft a formal Preparedness Doctrine for to determine key performance indicators for State agencies. Information hygiene practices, network and system assessments, and decision-making will comprise areas of special scrutiny.

Concurrent preparedness and possible legislative activities which will focus on gaining private sector support may also require the State to develop market incentives. The purpose of these incentives would be to motivate companies to adopt additional security practices, request technical support from external sources, and join information-sharing groups.

4.0 RESPONSE – Build and maintain robust statewide cyber incident response capabilities

- 4.1. Refine and enhance internal response protocols for incidents involving state government systems and networks.
- 4.2. Develop and maintain effective multi-agency cyber incident response plans that outline how the State will respond to major attacks on public and private sector information technology networks and industrial control systems.
- 4.3. Coordinate the development and deployment of cyber incident response teams and other deployable resources.

The State of Indiana must be able effectively respond to cybersecurity incidents, regardless of the size, scope, complexity, and the target of attack. Building upon existing IOT response protocols, an expanded response plan for significant cyber incidents will be developed to address breaches of state government networks. The formal development of a cybersecurity Emergency Support Function will detail the roles of lead, coordinating, and supporting agencies active during the response to a major incident.

5.0 INFRASTRUCTURE – Bridge the gaps between people, technology, and resources

- 5.1. Develop, maintain, and enhance the capabilities and functionality of the IN-ISAC.
- 5.2. Establish a public-facing cybersecurity website that serves as a clearinghouse for information.
- 5.3. Engage in statewide cyber infrastructure mapping.

The priority of the State is to build and expand systems and network solutions that support the five mission areas of prevention, protection, mitigation, response, and recovery. As well as the corresponding NIST Function Areas. Technology is only part of the solution. Human factors are key components of any cybersecurity effort. Education and public outreach programs focused on improving individual behavior and information security practices are essential to any successful strategy implemented by the State.

6.0 ECONOMIC OPPORTUNITIES – Leverage business and economic opportunities related to information, critical infrastructure, and network security

- 6.1. Launch an aggressive public information campaign to promote State cybersecurity initiatives.
- 6.2. Promote the use of the Muscatatuck Urban Training Center and Camp Atterbury as a cyber training ranges to regional, national, and international stakeholders.
- 6.3. Leverage the considerable technological resources of state universities and Indiana-based corporations to develop next-generation cybersecurity initiatives and attract investment.

Public and private organizations within the State should be as optimistic about the continued growth of cybersecurity efforts as they are concerned about attacks. Indiana's cybersecurity workforce can look forward exponential growth and opportunity – *if* the State cultivates conditions that train and retain skilled workers, attracts investment, and secures a competitive advantage for cybersecurity companies. Promotion of Indiana's cybersecurity initiatives will produce a synergy to ensure the growth of information security businesses and facilities. These initiatives can also support a wide variety of skilled jobs for Hoosiers, and strengthen a culture of preparedness that is critical for the State.

The Muscatatuck Urban Training Center's potential as a "cyber range" is also drawing interest from US DHS, which is considering MUTC as a federal training facility for cybersecurity. Today, the State has an unprecedented opportunity to leverage the "cyber problem" and emerge as a leader in innovative approaches to cybersecurity policy and practice — thereby serving the State's public safety interests while also attracting investment and promoting economic growth.

Indiana Department of Homeland Security (IDHS)

Crit-Ex 16.1

March 2016

Crit-Ex 2016

Cyber-Power Disruption Tabletop Exercise

Situation Manual

March 2016

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

Preface

The Crit-Ex 2016 Series 1 Tabletop Exercise (TTX) is sponsored by the Indiana Department of Homeland Security (IDHS), Indiana Office of Technology, and the Indiana National Guard. This Situation Manual (SitMan) was produced with input, advice, and assistance from the Crit-Ex 2016 Series 1 TTX Planning Team, which followed guidance set forth by the U.S. Department of Homeland Security (DHS) Homeland Security Exercise and Evaluation Program (HSEEP).

This SitMan provides exercise participants with all the necessary tools for their roles in the exercise. It is tangible evidence of Indiana's commitment to ensure public safety through collaborative partnerships that will prepare it to respond to any emergency.

The Crit-Ex 2016 Series 1 TTX is an unclassified exercise. Control of exercise information is based on public sensitivity regarding the nature of the exercise rather than actual exercise content. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

All exercise participants should use appropriate guidelines to ensure proper control of information within their areas of expertise and protect this material in accordance with current jurisdictional directives. Public release of exercise materials to third parties is at the discretion of IDHS and the Crit-Ex 2016 Core Team and Steering Committee.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Handling Instructions

1. The title of this document is Crit-Ex 2016 *Series 1 Tabletop Exercise (TTX) Situation Manual (SitMan).*

2. Information gathered in this SitMan is designated as For Official Use Only (FOUO) and should be handled as sensitive information that is not to be disclosed. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate security directives. Reproduction of this document, in whole or in part, without prior approval from IDHS is prohibited.

3. Given the scenario, topics and personnel involved in the Crit-Ex Tabletop Exercise, some of the discussion topics may necessitate restrictions. While this exercise is engineered to elicit productive dialogue on capabilities, not vulnerabilities, conversation may touch on issues with implications for local, state, or national security. This may include unclassified information about an organization's operations, the unauthorized disclosure of which could adversely impact a public safety or welfare, the effectiveness of the organization's critical operations programs, or other operations essential to state or national interest.

4. At a minimum, the attached materials will be disseminated strictly on a need-to-know basis and, when unattended, will be stored in a locked container or area that offers sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise Overview

Exercise Name	Crit-Ex Cyber-Power Disruption Tabletop Exercise
Exercise Date, Time, and Location	March 3, 2016 10AM – 4PM Camp Atterbury, Indiana
Scope	This exercise is a facilitated tabletop exercise, planned for 6 hours. The exercise is intended to facilitate discussion surrounding cyberattack response, energy disruption response, and other issues related to the mitigation of a wide-scale power outage.
Mission Area(s)	Mitigation, Response & Recovery
Core Capabilities	Operational Coordination; Operational Communications; Information Sharing
Objectives	1. Discuss the ability to establish and maintain a unified and coordinated operational structure and process that integrates all critical stakeholders during a power outage. 2. Discuss the ability to communicate information in support of security, situational awareness, and operations by all means available, within the area of operations and among all response forces during a power outage. 3. Discuss the ability develop and maintain a common operating picture throughout the duration of a power outage by providing timely, accurate, and actionable information, intelligence, data, or knowledge among government and private-sector entities, as appropriate.
Threat or Hazard	Cyberattack Vector: Control Systems Malware
Scenario	A state-sponsored terrorist group executes a coordinated cyberattack on several power facilities throughout Indiana, resulting in a widespread and prolonged power outage.
Sponsor	Indiana Department of Homeland Security
Participating Organizations	Approximately 25 participating organizations and 35 players from the Indiana Department of Homeland Security; Indiana Office of Technology; Indiana National Guard; Indiana Utility Regulatory Commission; Indiana State Police; local Emergency Management Agencies; Water/Wastewater Utilities; Power Utilities. For a full list of participating organizations, see Appendix B.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Points of Contact

David Kane
Executive Director
Indiana Department of Homeland Security
302 W. Washington St., E208
Indianapolis, IN 46254
dkane@dhs.in.gov

Jennifer de Medeiros
Emergency Services Program Manager
Indiana Department of Homeland Security
302 W. Washington St., W246
Indianapolis, IN 46254
(317) 452-0380
jdemedeiros@dhs.in.gov

James McHugh
Infrastructure Protection Program Manager
302 West Washington Street, Room W246
Indianapolis, IN 46204
317-473-0353
jmchugh@dhs.in.gov

MAJ Stacy Kennedy Barker
Deputy J7 Exercise and Training
2002 S. Holt Road
Indianapolis, IN 46241
Office: 317-247-3300 X73206

Additional Information

Crit-Ex planners have designed this exercise to focus on the coordination between critical infrastructure owners and operators and their local and state emergency management. The suggested audience includes jurisdictional emergency management partners and critical infrastructure owners and operators.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Contents

Preface 1
Handling Instructions 2
Exercise Overview 3
Contents 5
Section 1: General Information 6
Background 7
Purpose 7
Scope 7
Exercise Objectives & Core Capabilities 8
Participants 9
Exercise Structure 9
Exercise Evaluation 10
Exercise Guidelines 10
Assumptions & Artificialities 10
Section 2: Exercise Summary & Scenario 11
Module 1: Incident Onset & Notification 12
Module 2: Response & Continuity of Operations 14
Module 3: Recovery 16
Section 3: Exercise Appendices 18
Appendix A: Exercise Schedule 19
Appendix B: Exercise Participants 20
Section 4: Informational Appendices 21
Appendix C: Background Information 22
Appendix D: Case Studies 24
Appendix F: Cybersecurity Glossary 26
Appendix G: Acronyms 29

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

SECTION 1: GENERAL INFORMATION

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Background

The idea that the United States is facing a "Cyber 9/11" is at the forefront of homeland security discourse. Like the rest of the country, Indiana has a short window of opportunity to prepare for a major cybersecurity incident that, if successful, could be as devastating as a major earthquake or tornado. The year 2015 has been groundbreaking for developing cross-sector partnerships, governance structure, and strategic programs necessary for preventing, protecting, mitigating, responding to and recovering from cyber incidents. The Indiana Department of Homeland Security (IDHS) has been working in close conjunction with the Indiana Office of Technology (IOT) and the Indiana National Guard (INNG) to lead a collaborative effort between government, private-sector, military, and academic stakeholders, as well as incorporating cyber research to enhance Indiana's cybersecurity posture.

Crit-Ex 2016 is the first of these cross-sector initiatives, designed for both the public and private sectors in order to improve understanding of cybersecurity posture and identify capability gaps. It will function as a series of tabletop and functional exercises that explore the intersection of cybersecurity and critical infrastructure, using scenarios in which a cyberattack on a critical asset leads to physical-world consequences. The project is designed to recur annually, allowing partners from different critical infrastructure sectors across Indiana to participate and improve their cyber defenses. This year's scenario will focus on power disruption response within the water/wastewater and power sectors, allowing participants to exercise their cybersecurity processes across all five phases of emergency management. As such, Crit-Ex 2016 will be a "first-of-its kind" project that catalyzes information sharing, training opportunities, partnerships, and response planning across the state.

Purpose

The purpose of this exercise is to:

- Increase the operational readiness of the local, state and federal partners to respond to a prolonged, wide-spread power outage caused by a cyberattack.
- Evaluate the ability of local, state and federal partners to identify and respond to cascading events in accordance with current policies, plans, and procedures if traditional communications are down.
- Identify successes, shortfalls, and areas for improvement in current policies, plans, and procedures.

Scope

This exercise emphasizes the role of local, state and federal agencies, water/wastewater utilities, and power utilities in response to a coordinated cyberattack that affects the entire State of Indiana.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise Objectives & Core Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific mission area(s). The objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

Exercise Objective	Core Capability
1. Discuss the ability to establish and maintain a unified and coordinated operational structure and process that integrates all critical stakeholders during a power outage.	Operational Coordination
2. Discuss the ability to identify and maintain partnership structures among response elements to support situational awareness, mobilize critical resources, and establish coordination structures at the local, state, and national level.	Operational Coordination
3. Discuss the ability to communicate information in support of security, situational awareness, and operations by all means available, within the area of operations and among all response forces during a power outage.	Operational Communications
4. Discuss the ability to re-establish sufficient communications infrastructure within the affected areas to support critical services and transition to recovery.	Operational Communications
5. Discuss the ability to develop and maintain a common operating picture throughout the duration of a power outage by providing timely, accurate, and actionable information, intelligence, data, or knowledge among government and private-sector entities, as appropriate.	Information Sharing

Table 1. Exercise Objectives and Associated Core Capabilities

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Participants

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Players respond to the situation presented, based on expert knowledge of response procedures, current plans and procedures, and insights derived from training.

- **Observers:** Observers support the group in developing responses to the situation during the discussion; they are not participants in the moderated discussion period, however.

- **Facilitators:** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts during the TTX.

- **Evaluators:** Evaluators are assigned to observe and evaluate certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to written and established procedures.

- **Scribes:** Scribes are assigned to observe, listen, and record the participant discussions during the table group facilitated sessions.

Exercise Structure

This will be a multimedia, facilitated TTX. Players will participate in the following modules:

- **Module 1:** Incident Onset & Notification
- **Module 2:** Response
- **Module 3:** Recovery

Each module will begin with a multimedia update that summarizes key events occurring within that time period. After the updates, participants will review the situation and engage in functional group discussions of appropriate response issues. For this TTX, the functional groups are:

- Emergency Management
- Water/Wastewater Utilities
- Energy Utilities

After these functional group discussions, participants will engage in a facilitated caucus discussion in which a spokesperson from each group will present a synopsis of the group's actions based on the scenario.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise Evaluation

Evaluation of the TTX is based on a set of objectives and Exercise Evaluation Guides (EEGs). Evaluators will be provided with EEGs for each of their assigned areas, and players will be asked to complete exercise evaluation forms. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and compile the After Action Report (AAR).

Exercise Guidelines

- This TTX will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond on the basis of your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve response and preparedness efforts. Problem-solving efforts should be the focus.

Assumptions & Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted. During this exercise, the following apply:

- The scenario as designed may not be catastrophic or coordinated enough to cause a power outage that affects all the organizations involved. However, it is the intent of the Exercise Planning Team to utilize a catastrophic scenario according to Homeland Security Exercise and Evaluation Program (HSEEP) standards to drive exercise discussion.
- Incident attribution may take longer than the scenario describes. However, productive discussion will hinge on knowing the attack source and vector.
- There is no hidden agenda, and there are no trick questions.
- All players receive information at the same time.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

SECTION 2: EXERCISE SUMMARY & SCENARIO

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Module 1: Incident Onset & Notification

Date: Friday, January 15 – 5:00AM
Weather: Frigid winter weather. 15°F, 11 MPH winds NE

Over the course of several years, a hostile Nation State has sponsored individuals to work in electric generation facilities and control centers, where they had access to SCADA systems controlling both transmission and generation. These individuals have overcome the "air gap" (see Appendix) defense mechanisms by bridging the SCADA network and the business network. USB drives were used to install Remote Access Trojans (RATs) on all of the SCADA systems. The bridging laptops would then be used to connect to the RATs. The individuals now have remote control of both the generation SCADA system and the transmission SCADA system. Additional software was loaded that would erase evidence of the RATs.

At 5:00AM on January 15th, timed, coordinated cyberattacks are executed against these power facilities' generation control systems and transmission SCADA systems. These individuals begin opening breakers and changing generator setpoints to cause the generators to go into an overspeed condition and trip offline. The result is immediate power disruption across approximately 70% of the state, with outages extending outside state lines.

Within 30 minutes, cascading effects visibly impact the interdependencies of the facilities. Traditional communication lines are disrupted, including telecommunications and cell towers. Most of the state is blind to the coordinated nature of the incident and the extent of the outages.

Key Issues

- Indiana is experiencing a power loss that covers nearly 70% of the state and surrounding region.
- Throughout the powerless region, telecommunications circuits fail and/or are jammed.
- Power outage alarms alert water/wastewater facilities of the power outage.
- Not every jurisdiction is aware that a cyber-attack has caused this power outage and most are going through normal power outage recovery operations.

Questions

The following questions are provided as suggested general subjects. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

- What actions would your organization take initially? What are your organization's first priorities?
- Who is your first call? How do you identify your critical partners for a power outage?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

- How would you contact partners outside the organization without traditional communications? Within the organization? What is the primary and alternate (backup) method to notify personnel about the status of your organization and its needs?
- How will the information presented in the scenario be shared? Who is contacted as part of the alert/notification process—are pre-identified key personnel notified, and are other State agencies notified?
  - Local Government, Police, Fire, Emergency Services, and trusted third parties?
  - State partners and/or agencies?
  - Federal partners and/or agencies?
- Based on your contact and alert procedures after an incident, do those match your mandated reporting requirements? Internal? Local, state, and federal levels of government? What specifically are your reporting requirements?
- How do you determine when and with whom to share sensitive and/or classified information about the event, including information about proprietary systems? What concerns or considerations do you have in coordinating with or discussing your situation with external entities?
- What are the backup power requirements for your agency? How long could you sustain operations from your primary facility on generators/backup power?
  - When was the last time these backup systems were checked and/or tested? (e.g., fuel, maintenance, etc.)
- What resources and capabilities are available to analyze or deal with the disruption? Do you have pre-defined cyber incident response teams? What external resources would you use?
- Based on the scenarios identified and from where you sit now, do you see any voids or vacuums in either the private and/or public sectors that should be better managed, enhanced, or filled? (e.g. "*I believe the state can do a better job of X, Y, and Z*" or "*I believe a sector does a poor job of prior planning regarding X, Y, and Z.*")

Related Objectives

- Assess the effectiveness of the organization's incident reporting and notification process.
- Determine how and how quickly utilities communicate with interdependent facilities, emergency management and government following an attack.
- Identify when intelligence and information is shared, and with whom.
- Identify available resources and resource request channels for a power outage.
- Explore the timelines and communication channels for power disruption incident management.
- Explore what polices and/or procedures are in place to identify a cyber-incident.
- Explore what policies and/or procedures are in place to react and mitigate a cyberattack

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Module 2: Response & Continuity of Operations

Date: Friday, January 15 – 9:00AM through Tuesday, January 19 – 5:00PM
Weather: Between 13°F and 25°F, depending on location

While conducting normal procedural recovery operations, IT personnel discover that malware has infected all forms of back up, preventing any restoration capabilities on those systems at this moment in time. By noon, a state-sponsored terrorist group claims responsibility for the cyberattack. State officials are now aware of the complexity surrounding the attack causing widespread outages over the region. State officials are now aware of the complexity surrounding this attack causing widespread outages over the region.

Some rural locations outside immediate downtown have power, but the certainty of that power maintaining is unknown. Many employees are stranded at home, unaware of the catastrophe caused by this cyberattack. Local counties conducting response operations are beginning to request government assistance, with heated shelters at the top of their list. Given the frigid winter temperatures, heat will become a life-dependent commodity along with food and water.

Water utilities are starting to feel the strain of the attack affecting their ability to provide service to its customers. The weather could have cascading effects on the water supply if the lack of power disrupts the ability of the utility companies to keep water from freezing. Within 24 hours, local fuel supplies will begin to dry up because of increased use for power generators. There are also signs of looting in the powerless regions, with the general public still unware of how serious the power outage is.

The private-sector operations dependent upon information technology and/or power have shut down or transitioned to alternate methods. Utility companies without proper continuity of operations plans are moving very slow in their transition to manual operations in an attempt to get the power back on.

Key Issues

- Power is still out in the downtown area and significant islanding around the state and region. Systems cannot be restored from backup.
- Terrorists have claimed responsibility for the cyberattack.
- Freezing temperatures pose a public safety issue and affect pipes.
- Communication issues plague the utility sector.
- Fuel availability for transportation and generators will become an issue in the immediate future.

Questions

The following questions are provided as suggested general subjects. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

- How and with whom will this information be communicated?
- Does this information change your priorities? How? How will it affect your response operations? How would a law enforcement investigation impact your current operations?
- How does the attribution of a terrorist cyberattack change your priorities and courses of action?
- What types of sensitive information/intelligence need to be communicated outside your organization, and how will that be delivered?
- Does your organization have the resources it needs to respond to this cyberattack? How will you request more resources?
- What protective actions would you take across non-impacted systems or agencies?
  - Who is responsible for protective action decision-making?
  - How are actions coordinated across departments/agencies?
- What external resources would be needed to support the response and continue your mission-essential functions (MEFs) and primary mission-essential functions (PMEFs)?
- What mutual aid agreements does your organization partake in? Are processes in place to request government or third party resources? Do current mutual aid agreements or assistance request processes address power-disruption resources and staff?
- What if key personnel are unavailable due to lack of notification or inability to reach the facility? What is each entities alternate approach to staffing? Would this degrade your ability to perform MEFs?
- Does your entity have backup power-generation capabilities for an extended blackout period? If not, how will you address the issue? What other contingency plans are required to address an extended blackout period?
- How will you address public safety issues? With what agencies/entities will you coordinate?
- What plans, procedures, and/or agreements do you have in place to control resource distribution within and outside your jurisdiction?

Related Objectives

- Assess the effectiveness of the organization's secondary communications capabilities.
- Examine the effectiveness of the organizations intelligence information-sharing protocols.
- Analyze the organization's ability to coordinate with external organization to access resources to respond to the attack and power outage.
- Determine primary and alternate sources for response capabilities.
- Identify the second and third-order effects of a prolonged power outage both at the organization and its partners.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Module 3: Recovery

Date: January 20, 11:00AM ongoing
Weather: Between 17°F and 30°F, depending on location

ICS-CERT, SCADA incident response teams, and other private-sector cybersecurity experts have started to eradicate the malware from the control systems so that normal operations can continue. Private-sector critical infrastructure providers begin to restore service as quickly as possible, starting with the Indy Metro area. Providers with advanced planning efforts are able to restore service quicker than others, but some of the critical infrastructure requiring replacement is in limited supply. This depleted supply chain will have continuing affects resulting in limited power supply in certain regions of Indiana until the entire infrastructure is revived.

The local population is now aware of the cyberattack affecting power to their regions. Local law enforcement and emergency teams have been placed throughout the region, providing continual support to those who are still lacking power. Many people have been displaced during the power outage and will now need to be transported back to their dwellings. The terrorist group has continued to boast of their accomplishment on social media, warning that any region in the United States with similar industrial control networks will become a target in the future.

Key Issues

- Power and essential services are beginning to be restored.
- The governor has directed all agencies to return to normal operations
- Limited supply on critical infrastructure replacement parts and/or systems
- Many of the populace is still without power and/or been removed from their homes for safety reasons.
- Public opinion could swing negatively given the terrorist social media presence.

Questions

- Describe your role in post-incident recovery.
- At what point does your organization decide that it is in recovery mode? How would your organization support the transition back to a normal operating state?
  - How would you work with critical infrastructure providers to determine the incident is over?
- What processes or protocols are in place when contacting and/or working with law enforcement?
- How do you prioritize the allocation of critical infrastructure parts and/or systems? How are they distributed?
- Who are the essential personnel in a recovery mode? What are your organization's key coordination points at this time?
- How do you prioritize where to allocate resources?
- What external resources would be needed to support the recovery? When do mutual aid compacts end?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

- What external resources would be needed to support continuous recovery? Are processes in place to request government and/or third party resources? How would these resources be distributed?
- Describe the process for how your agency would capture mission-critical findings; lessons learned; shortfalls; and gaps in plans, policies, and procedures to improve COOP.
- How would you address any misinformation in the media?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

SECTION 3: EXERCISE APPENDICES

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix A: Exercise Schedule

March 3, 2016 Time	Activity
9:15	Registration
10:00	Welcome & Opening Remarks
10:30	TTX Overview
10:45	Module One & Questions
10:55	Break-Out Sessions
11:45	Working Lunch & Module One Discussion
12:45	Module Two & Questions
12:55	Breakout Sessions
1:40	Module Two Discussion
2:00	Break
2:10	Module Three & Questions
2:20	Breakout Sessions
3:05	Module Three Discussion & Hotwash
3:50	Closing Remarks

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix B: Exercise Participants

Participating Organizations
Indiana Department of Homeland Security
Infragard Indiana
FEMA Region V
Indiana Office of Technology
Indiana Army National Guard
Indiana Utility Regulatory Commission
Indiana State Police
Allen County EMA
Bartholomew County EMA
Crawford County EMA
Montgomery County EMA
Vanderburgh County EMA
US Department of Homeland Security
Federal Bureau of Investigation
Michigan City Water
Evansville Water & Sewage
Fort Wayne Utilities
Citizens Energy Group
Vectren
Duke Energy
AES/Indianapolis Power & Light
NiSource/NIPSCO
Indiana Michigan Power Company
Rook Security
MISO
Pondurance

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

SECTION 4: INFORMATIONAL APPENDICES

The following section includes background and example information related to cybersecurity threats and attacks on the power grid.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix C: Background Information

Air Gap

An air-gapped computer is one that is neither connected to the Internet nor connected to other systems that are connected to the Internet. Air gaps generally are implemented where the system or network requires extra security, such as classified military networks or industrial control systems (ICS) that operate critical infrastructure. To maintain security, ICS should only be on internal networks that are not connected to the company's business network, thus preventing intruders from entering the corporate network through the Internet and working their way to sensitive systems. A true air gap means the machine or network is physically isolated from the Internet, and data can only pass to it via a USB flash drive, other removable media, or a firewire connecting two computers directly.

Many companies insist that a network or system is sufficiently air-gapped even if it is only separated from other computers or networks by a software firewall. However, these firewalls can be breached if the code has security holes or if the firewalls are configured insecurely. Although air-gapped systems were believed to be more secure in the past, recent attacks involving malware that spread via infected USB flash drives have showcased vulerabilities. More recently, evidence has shown that air-gapped systems can also be attacked through radio waves.

BlackEnergy Malware

BlackEnergy was first identified several years ago as a type of malware used to launch distributed denial of service attacks (DDoS) and steal information. The majority of BlackEnergy's computer coding appears designed to conduct highly sophisticated monitoring and recording of data – a tactic known as "sniffing." However, more recent versions of BlackEnergy, such as BlackEnergy3, have evolved into an advanced persistent threat (APT) tool used in significant geopolitical operations, including Russia, Poland and most recently Ukraine.

Experts worry that versions of BlackEnergy could be programmed to damage pieces of critical infrastructure by hacking into its control system, since its complexity hints at a highly skilled team of hackers with a broad technical background. This latest version of BlackEnergy is "modular," making it much easier for hackers to quickly change how the malware works, and significantly harder for security analysts to find and root it out.

Also worrisome is the proliferation of BlackEnergy malware. The US Department of Homeland Security has already identified BlackEnergy malware deep within the industrial control systems that operate critical infrastructure, and evidence is mounting that the bug has already been deployed around Europe and is "sleeping" until activated. Cybersecurity analysts say they are sure the bug will continue to spread, and that will lead to many more blackouts and "mysterious" malfunctions in national power grids, transportation, and other industrial infrastructure.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Remote Access Trojans

Remote Access Trojans (RATs) provide cybercriminals with unlimited access to infected endpoints. Using the victim's access privileges, they can access and steal sensitive business and personal data – including intellectual property and personally identifiable information. While automated cyberattacks allow cybercriminals to attack browser-based access to sensitive applications, RATs are used to steal information through manual operation of the endpoint on behalf of the victim. Most Advanced Persistent Threat (APT) attacks take advantage of RAT technology for reconnaissance, bypassing strong authentication, spreading the infection, and accessing sensitive applications to exfiltrate data. RATs are commercially available (e.g. Poison Ivy, Dark Comet) and can be maliciously installed on endpoints using drive-by-download and spearphishing tactics.

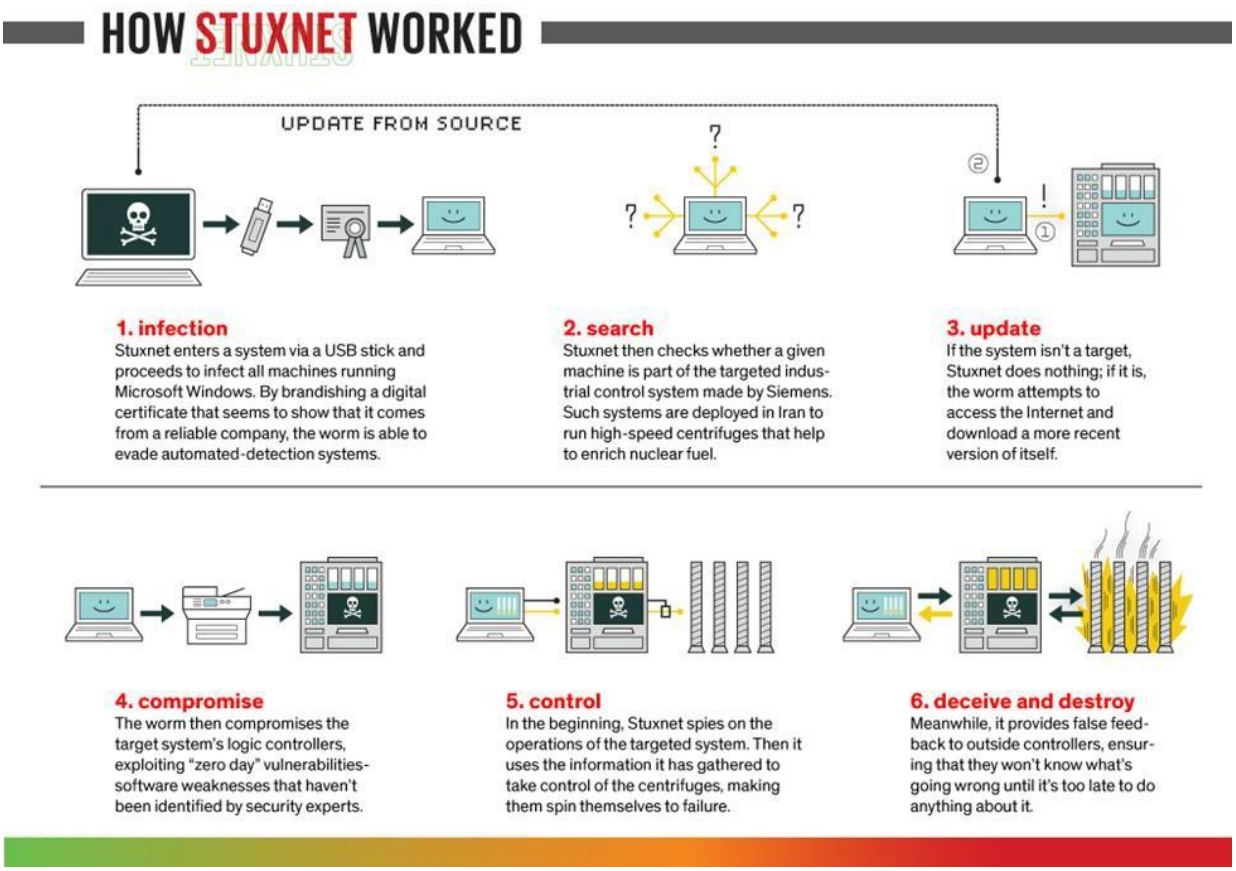
NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix D: Case Studies

Stuxnet

One of the most famous cases involving the infection of an air-gapped system is Stuxnet, the virus/worm designed to sabotage centrifuges used at a uranium enrichment plant in Iran.

Although a computer virus relies on an unwitting victim to install it, a worm spreads on its own, often over a computer network. First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself. Then it sought out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment, such as centrifuges. Finally, it compromised the programmable logic controllers – the heart of a SCADA system. The worm's authors could thus spy on the industrial systems and even cause the fast-spinning centrifuges to tear themselves apart, unbeknownst to the human operators at the plant.
.



NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Shamoon
The most destructive post-Stuxnet discovery of advanced threats is a malicious malware known as Shamoon. Like Stuxnet, Duqu and Flame, it targeted energy companies in the Middle East, this time Saudi Aramco, Qatar's RasGas and other oil and gas concerns in the region.

Shamoon was introduced into Saudi Aramco by a disgruntled insider who had full access to the system. It took control of an Internet connected computer and used that computer to communicate back to an external Command-and-Control server. It also infected other computers that were not Internet connected. This type of malware is called a "botnet," which is a collection of compromised computers under the control of a single individual or group. While it did not disrupt an industrial process or stealthily steal business information as previous types of malware did, Shamoon removed and overwrote the information on the hard drives of 30,000 to 55,000 workstations of Saudi Aramco, wiping the computers' hard drives clean.

Saudi Aramco says damage was limited to office computers and did not affect systems software that might hurt technical operations. However, the destruction of 30,000 workstations undoubtedly caused a vast amount of damage without directly hitting oil production or harming the flow of oil out of the ground.

Ukrainian Cyberattack
On December 23, 2015, Western Ukrainian power company Prykarpattyaoblenergo reported an outage on December 23rd that affected an area including the regional capital Ivano-Frankivsk. A subsequent investigation revealed that a variant of the BlackEnergy malware had caused "interference" in the working of the company's systems, which led to the power interruption. The investigation also found that the malware had been injected into the networks of two other utilities, though neither had reported any service problems. This event is a milestone because, while destructive events have been targeted at energy before – oil firms, for instance – this is the first event that has caused the widely feared blackout.

BlackEnergy used Microsoft Office documents containing malicious macros in these particular attacks. The attack scenario is simple: the target receives a spearphishing email that contains an attachment with a malicious document. The document itself contains text trying to convince the victim to run the macro in the document. This is an example where social engineering is used instead of exploiting software vulnerabilities. If victims are successfully tricked, they end up infected with BlackEnergy Lite.

German Steel Mill Cyberattack
In December 2014, the German government's Federal Office for Information Security released an annual findings report in which they noted that a malicious actor had infiltrated a steel facility. The adversary used a spearphishing email to gain access to the corporate network and then moved into the plant network. According to the report, the adversary showed extensive knowledge in industrial control systems (ICS) and was able to cause multiple components of the system to fail. This specifically caused critical process components to become unregulated, which resulted in massive physical damage. To date, the only other public example of a cyberattack causing physical damage to control systems was Stuxnet.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix F: Cybersecurity Glossary

Access control: The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Advanced Persistent Threat: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

Alert: A notification that a specific attack has been detected or directed at an organization's information systems.

Antivirus software: A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents – sometimes by removing or neutralizing the malicious code.

Blue Team: A group that defends an enterprise's information systems when mock attackers (i.e., the Red Team) attack, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group (i.e., the White Team).

Bot: A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under the command and control of a remote administrator.

Bot master: The controller of a botnet that, from a remote location, provides direction to the compromised computers in the botnet**.**

Computer network defense: The actions taken to defend against unauthorized activity within computer networks.

Continuity of Operations Plan: A document that sets forth procedures for the continued performance of core capabilities and critical operations during any disruption or potential disruption.

Cyber ecosystem: The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.

Cyber infrastructure: An electronic information and communications systems and services and the information contained therein.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Denial of Service: An attack that prevents or impairs the authorized use of information system resources or services.

Distributed Denial of Service (DDoS): A denial of service technique that uses numerous systems to perform the attack simultaneously.

Encryption: The process of transforming plaintext into ciphertext.

Firewall: A capability to limit network traffic between networks and/or information systems.

Hacker: An unauthorized user who attempts to or gains access to an information system.

Industrial Control System: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets.

Inside(r) threat: A person or group of persons within an organization who pose a potential risk through violating security policies.

Keylogger: Software or hardware that tracks keystrokes and keyboard events, usually surreptitiously / secretly, to monitor actions by the user of an information system.

Malicious code: Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Passive attack: An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Penetration testing: An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Phishing: A digital form of social engineering to deceive individuals into providing sensitive information.

Remote-Access Trojan: A malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program or sent as an email attachment.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Red Team: A group authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's cybersecurity posture.

Spyware: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

Supervisory Control and Data Acquisition: A generic name for a computerized system that is capable of gathering and processing data and applying operational controls to geographically dispersed assets over long distances.

Threat: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

Trojan horse: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

White Team: A group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix G: Acronyms

AAR: After action report

APT: Advanced persistent threat

DDoS: Distributed denial of service

DHS: Department of Homeland Security

EEG: Exercise evaluation guide

EMA: Emergency management agency

FOUO: For Official Use Only

HSEEP: Homeland Security Exercise & Evaluation Program

ICS: Industrial control system

IDHS: Indiana Department of Homeland Security

INNG: Indiana National Guard

IOT: Indiana Office of Technology

MEF: Mission essential function

PMEF: Primary mission essential function

POC: Point of contact

RAT: Remote-Access Trojan

SCADA: Supervisory Control & Data Acquisition

SitMan: Situation manual

TTX: Tabletop exercise

USB: Universal Serial Bus

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Indiana Department of Homeland Security (IDHS)

Crit-Ex 16.2

May 2016

Crit-Ex 16.2

Water Utility Disruption Facilitated Cyber Exercise

Exercise Plan

May 18-19, 2016

This Exercise Plan (EXPLAN) provides participants with all the necessary tools for their roles in the exercise. Use of the EXPLAN by all exercise participants is unrestricted.

Preface

The Crit-Ex 2016 Series 2 (Crit-Ex 16.2) Facilitated Cyber Exercise is sponsored by the Indiana Department of Homeland Security (IDHS), Indiana Office of Technology, and the Indiana National Guard. This Exercise Plan (EXPLAN) was produced with input, advice, and assistance from the Crit-Ex 16.2 Planning Team, which followed guidance set forth by the U.S. Department of Homeland Security (DHS) Homeland Security Exercise and Evaluation Program (HSEEP).

This EXPLAN provides exercise participants with all the necessary tools for their roles in the exercise. It is tangible evidence of Indiana's commitment to ensure public safety through collaborative partnerships that will prepare it to respond to any emergency.

The Crit-Ex 16.2 Facilitated Cyber Exercise is an unclassified exercise. Control of exercise information is based on public sensitivity regarding the nature of the exercise rather than actual exercise content. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the EXPLAN.

Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Handling Instructions

1. The title of this document is Crit-Ex 16.2 *Cyber Exercise Plan (EXPLAN).*

2. Information gathered in this EXPLAN is designated as For Official Use Only (FOUO) and should be handled as sensitive information that is not to be disclosed. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate security directives. Reproduction of this document, in whole or in part, without prior approval from the exercise sponsors is prohibited.

3. Given the scenario, topics, and personnel involved in the exercise, some of the discussion topics may necessitate restrictions. While this exercise is engineered to elicit productive dialogue on capabilities, not vulnerabilities, conversation may touch on issues with implications for local, state, or national security. This may include unclassified information about an organization's operations, the unauthorized disclosure of which could adversely impact public safety or welfare, the effectiveness of the organization's critical operations programs, or other operations essential to state or national interest.

4. At a minimum, the attached materials will be disseminated strictly on a need-to-know basis and, when unattended, will be stored in a locked container or area that offers sufficient protection against theft, compromise, inadvertent access, and unauthorized disclosure.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise Overview

Exercise Name	Crit-Ex 16.2 Water Utility Disruption Facilitated Cyber Exercise
Exercise Date, Time, and Location	May 18 and 19, 2016 8AM – 7PM Muscatatuck Urban Training Center, Indiana
Scope	This exercise is a controlled, operations-based, facilitated cyber exercise, planned for two 10 hour days of execution. The exercise is intended to bring awareness and discuss potential responses to a cyberattack on water utility Supervisory Control and Data Acquisition (SCADA) systems, and improve the overall security and responsiveness in the event that an advanced cyber event disrupts essential utility services and presents debilitating effects across a range of critical functions.
Mission Areas	Mitigation, Response, and Recovery
Core Capabilities	Operational Coordination, Operational Communications, Intelligence and Information Sharing, and Cybersecurity
Objectives	1. Protect and restore the SCADA system information and services from damage, unauthorized use, and exploitation caused by malicious activity. 2. Stabilize water infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community. 3. Bring awareness to the current readiness of water utilities to respond to a cyberattack and draw out best practices for improving system security and incident response. 4. Provide water utility observers with the training that empowers them for a real-world emergency, identifying key decision points, and decision making.
Threat or Hazard	Cyberattack Vector: Control Systems Malware
Scenario	A state-sponsored terrorist group (Red Team) remotely conducts a cyberattack on a SCADA system at various water utility treatment facilities in Indiana with the identified utility representatives (Blue Team) serving as active observers.
Sponsors	Indiana Department of Homeland Security, Indiana Office of Technology, Indiana Army National Guard

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Participating Organizations	Approximately 16 participating organizations and 18 players from the Indiana Department of Homeland Security; Indiana Office of Technology; Indiana National Guard; Indiana water/wastewater utilities, the Indiana Chapter of the AWWA, Indiana Energy Association, and cybersecurity organizations. For a full list of participating organizations, see Appendix D.
Points of Contact	Jennifer de Medeiros Emergency Services Program Manager Indiana Department of Homeland Security 302 W. Washington St., W246 Indianapolis, IN 46254 (317) 452-0380 jdemedeiros@dhs.in.gov James McHugh Critical Infrastructure Program Manger 302 West Washington Street, Room W246 Indianapolis, IN 46204 317-473-0353 jmchugh@dhs.in.gov Doug Rapp President, Cyber Leadership Alliance 85 East Cedar Street Zionsville, IN 46077 doug@cyberleaders.org Philip N. Barker Contractor, Patriot Strategies Program Manager Atterbury-Muscatatuck Center for Complex Operations Office: (317) 247-3300 ext.: 62063 Cell: (812) 345-4343 philip.n.barker.ctr@mail.mil
Additional Information	Crit-Ex 16.2 planners have designed this exercise to focus on water utility cyberattack management. The suggested audience should be limited to water utilities, cyber-incident response entities, and government.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Contents

Preface 2
Handling Instructions 3
Exercise Overview 4
Contents 6
Section 1: General Information 7
Background 8
Purpose 8
Scope 9
Core Capabilities & Exercise Objectives 9
Participants 12
Exercise Structure 13
Exercise Evaluation 13
Exercise Guidelines 13
Assumptions & Artificialities 14
Section 2: Exercise Summary & Scenario 15
Systems/Network Overview 16
Attack Vectors and Desired Effects 17
Exercise Scenario Background 17
Phase 1: "Business As Usual" 17
Phase 2: "Fool Me Twice" 19
Phase 3: After Action Review 21
Section 3: Exercise Appendices 22
Appendix A: Exercise Schedule 23
Appendix B: Core Capability/AWWA Practice Standards Crosswalk 25
Appendix C: Atterbury-Muscatatuck Map 29
Appendix D: Exercise Participants 30
Appendix E: Exercise Planning Team Members 31
Section 4: Information Appendices 33
Appendix F: Background Information 34
Appendix G: Case Studies 36
Appendix H: Cybersecurity Glossary 38
Appendix I: Acronyms 41

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

SECTION 1: GENERAL INFORMATION

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Background

The idea that the United States is facing a "Cyber 9/11" is at the forefront of homeland security discourse. Like the rest of the country, Indiana has a short window of opportunity to prepare for a major cybersecurity incident that, if successful, could be as devastating as a major earthquake or tornado. The year 2016 has been groundbreaking for developing cross-sector partnerships, governance structure, and strategic programs necessary for preventing, protecting, mitigating, responding to and recovering from cyber incidents. IDHS has been working in close conjunction with the Indiana Office of Technology (IOT) and the Indiana National Guard (INNG) to lead a collaborative effort between government, private-sector, military, and academic stakeholders, as well as incorporating cyber research to enhance Indiana's cybersecurity posture.

Crit-Ex 2016 is the first of these cross-sector initiatives, designed for both the public and private sectors in order to improve understanding of cybersecurity posture and identify capability gaps. It will function as a series of tabletop, demonstration, and functional exercises that explore the intersection of cybersecurity and critical infrastructure, using scenarios in which a cyberattack on a critical asset leads to physical-world consequences. The project is designed to recur annually, allowing partners from different critical infrastructure sectors across Indiana to participate and improve their cyber defenses. This year's scenarios are focusing on cyberattacks disrupting SCADA systems at a water and power utility, allowing participants to exercise their cybersecurity response processes. As such, Crit-Ex 2016 will be a "first-of-its kind" exercise that catalyzes information sharing, training opportunities, partnerships, and response planning across the state.

Purpose

The purpose of the Crit-Ex 16.2 Cyber Exercise is to improve the overall security and responsiveness of Indiana's critical infrastructure in the event that an advanced cyber event disrupts essential services, and presents debilitating effects across a range of critical functions. Crit-Ex 16.2 will also:

- Increase key stakeholder awareness to a cyberattack on a water utility SCADA system;
- Improve the overall security and responsiveness in the event that an advance cyber event disrupts essential utility services and presents debilitating effects across a range of critical functions;
- Offer a real-world simulation of a small rural water company and provide a learning opportunity to improve SCADA security and operations;
- Develop security technologies and best practices for the field devices based upon actual and expected Industrial Control Systems (ICS) cyber incidents; and
- Establish, promote, and support an open demonstration facility at Muscatatuck Urban Training Center (MUTC), and additional areas around the State that are dedicated to, and promote best practices for ICS systems.

.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Scope

This exercise focuses on how water/wastewater utilities will respond to a coordinated cyberattack, and also draws the role of federal, state, and local agencies into the conversation. This exercise will be a controlled, operations-based facilitated cyber exercise, planned for two, 10 hour days of execution. The exercise will bring awareness of and discuss potential responses to a cyberattack.

Core Capabilities and Exercise Objectives

The National Preparedness Goal of September 2011 has steered the focus of homeland security toward a capabilities-based planning approach using 32 identified Core Capabilities. Capabilities-based planning focuses on planning under uncertainty because the next disaster can never be forecast with complete accuracy. Therefore, capabilities-based planning takes an all-hazards approach to planning and preparation that builds capabilities, which can be applied to a wide variety of incidents. States and urban areas use capabilities-based planning to identify a baseline assessment of their homeland security efforts by comparing their current capabilities against the Core Capabilities. This approach identifies gaps in current capabilities.

The Core Capabilities are essential for the execution of each of the five mission areas: Prevention, Protection, Mitigation, Response, and Recovery. These capabilities provide the foundation for development of the exercise design objectives and scenario.

Mitigation Mission Area: Mitigation comprises “the capabilities necessary to reduce the loss of life and property by lessening the impact of disasters.”

Response Mission Area: Response comprises “the capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.”

Recovery Mission Area: Recovery comprises "the core capabilities necessary to assist communities affected by an incident to recover effectively.”

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to both the identified Core Capabilities and the American Water Works Association’s (AWWA) standards. The Core Capabilities are identified as distinct critical elements necessary to achieve the specific mission area(s) and the AWWA Practice Categories are recommended cybersecurity practices for the Water Sector. The objectives, aligned Core Capabilities and AWWA Practice Categories were selected by the Exercise Planning Team. Appendix B of this EXPLAN provides a more detailed breakdown of the crosswalk between Core Capabilities and AWWA Practice Standards.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise Objective	Core Capability	AWWA Practice Standards
1. Protect and restore the SCADA system information and services from damage, unauthorized use, and exploitation caused by malicious activity.	• Cybersecurity (CS), • Intelligence & Information Sharing (I/IS) • Operational Coordination (OC)	• Access Control (CS) • Application Security (CS) • Business Continuity & Disaster Recovery (OC, OS) • Education (CS) • Encryption (CS) • Government and Risk Management (OC, CS) • Operations Security (CS) • Personnel Security (CS) • Physical Security of PCS Equipment (CS) • Server and Workstation Hardening (CS) • Service Level Agreements (CS) • Telecom, Network Security, and Architecture (CS)
2. Stabilize water infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.	• Operational Coordination (OC) • Operational Communications (OCOM)	• Access Control (OC) • Business Continuity & Disaster Recovery (OC) • Encryption (OCOM)) • Governance and Risk Management (OC) • Service Level Agreements (OC, OCOM) • Telecommunications, Network Security, and Architecture (OCOM))

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

3. Bring awareness to the current readiness of water utilities to respond to a cyberattack and draw out best practices for improving system security and incident response.	• Cybersecurity (CS) • Operational Coordination (OC) • Operational Communications (OCOM)	• Access Control (CS) • Application Security (CS) • Business Continuity and Disaster Recovery (CS, OC, OCOM) • Education (CS, OCOM) • Encryption (CS, OCOM) • Governance and Risk Management (CS, OC) • Operations Security (CS) • Personnel Security (CS) • Physical Security of PCS Equipment (CS) • Service Level Agreements (CS, OCOM) • Service and Workstation Hardening (CS) • Telecommunications, Network Security, and Architecture (CS)
4. Provide water utility observers with the training that empowers them for a real world emergency, identifying key decision points and decision making.	• Cybersecurity (CS), • Intelligence & Information Sharing (I/IS)	• Access Control (CS) • Application Security (CS) • Business Continuity and Disaster Recovery (CS) • Encryption (CS) • Governance and Risk Management (CS) • Operations Security (CS) • Personnel Security (CS) • Physical Security of PCS Equipment (CS) • Server and Workstation Hardening (CS, IS) • Service Level Agreements (CS) • Telecommunications, Network Security, and Architecture (CS, IS) • Education (CS, IS)

Table 1. Exercise Objectives and Associated Core Capabilities/AWWA Standards

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Participants

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Players respond to the situation presented, based on expert knowledge of response procedures, current plans and procedures, and insights derived from training.

- **Controllers:** The exercise control representative is trained on the specifics of the exercise, to include the MSEL and evaluation criteria. This individual will help to guide the exercise as needed to ensure that it meets the training intent, and records data that will be evaluated against exercise/industry best practices.

- **Observers:** Observers support the group in developing responses to the situation during the discussion; however, they are not participants in the moderated discussion period. For this exercise the planning team has additionally identified the role of utility observer, with specific roles to include the following:
    - **Utility Observer:** This participant is a member of the utility team and is generally familiar with utility response plans and the expectations of the utility leadership. The Utility Observer will be situated in the Control Room and observer operations during exercise execution.

- **Facilitators:** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts during the Exercise. For this exercise representatives from Purdue and Indiana University are scheduled to serve in this role.

- **Exercise Operator:** The exercise operator is a non-participating member of the team who is familiar with the environment/controls that are being used in the exercise. Individuals in this role will be utilized to be an interpreter for the environment, and an extension of the controls for a utility operator who may not be comfortable at the controls in an unfamiliar operating environment.

- **Utility Operator/Supervisor:** The utility operator is the individual who physically sits at the controls of the plant and has intimate knowledge of water treatment operations. The supervisor intimately understands water treatment operations and is most familiar with incident management procedures for the utility and will potentially go into the field during exercise execution. Depending on the size and structure of the specific utility, the utility operator and utility supervisor might be the same individual.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

- **Evaluators:** Evaluators are assigned to observe and evaluate certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to written and established procedures.

- **VIPs:** VIPs are individuals who have been invited to the exercise event, but will be in attendance briefly and do not serve any official role in exercise conduct.

Exercise Structure

This will be a multimedia, facilitated Exercise. Wastewater utility observers ("players") will participate in the following exercise events/phases:

- **Phase 1:** "Business as Usual"
- **Phase 2:** "Fool Me Twice"
- **Facilitated After Action Review**

Each phase of the cyber exercise will begin with a multimedia update that summarizes key events occurring. After the updates, active observers will review the situation and engage in facilitated discussions of appropriate response issues. For Crit-Ex 16.2, the functional groups are:

- Operators
- Supervisors

After these functional group discussions, participants will engage in a facilitated After Action Review discussion in which representatives from each utility will present a synopsis of the group's actions based on the scenario presented.

Exercise Evaluation

Evaluation of the exercise is based on a set of objectives developed by the Exercise Planning Team. Evaluators will be provided with the identified objectives, and players will be asked to complete exercise evaluation forms. These documents, coupled with facilitator observations and notes compiled during the After Action Review process will be used to evaluate the exercise and compile the After Action Report (AAR).

Exercise Guidelines

- This Exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond on the basis of your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve response and preparedness efforts. Problem-solving efforts should be the focus.

Assumptions & Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted. During this exercise, the following apply:

- The scenario as designed may not be catastrophic or coordinated enough to affect all the organizations involved. However, it is the intent of the Exercise Planning Team to utilize a catastrophic scenario according to Homeland Security Exercise and Evaluation Program (HSEEP) standards to drive exercise discussion.
- Incident attribution may take longer than the scenario describes. However, productive discussion will hinge on knowing the attack source and vector.
- There is no hidden agenda, and there are no trick questions.
- All players receive information at the same time.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

SECTION 2: SYSTEMS/NETWORK OVERVIEW & EXERCISE SCENARIO BACKGROUND

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Systems/Network Overview

For Crit-Ex 16.2 the exercise will utilize a system specifically designed to mirror a small municipal water treatment plant. The water plant has two Allen Bradley MicroLogix Programmable Logic Controllers (PLC). One monitors turbidity of the filtered water, and the other controls the High Service pumps based on flow and/or pressure. These PLCs are connected through a Cisco process network to Human-Machine Interface (HMI) and data servers located in building 5016 using Rockwell Automation FactoryTalk View software. The plant operator uses an operator workstation (client) to monitor and control the water plant. Also located in the control room is a business personal computer (PC) connected to the Internet through an Integrated Threat Management appliance (SonicWALL). The third PC in play is a historian/engineering server. It is used to collect trended information and as a programming terminal with RSLogix software installed to modify the PLC code as required**.**

The operator control room will be equipped with several monitors including:

- Operator Workstation – What the operator sees on his HMI
- Business Workstation – Used for Internet access and email
- Engineering Workstation – PLC programming/engineering

A "mirrored server" is also connected to the PLCs. It will allow for the monitoring of actual plant control activities and feed information to the observation room during the breach. Screens will also be in-place to show the changes that occur within the PLC and the associated network traffic and event log changes that occur as result of the attack. To do this, the observation room will be equipped with monitors that include: (See Figure 2.1 for additional information)

1. Operator Workstation – What the operator sees on his HMI
2. Observer Workstation – Actual (reality) HMI values from the water plant's PLC
3. Wireshark – real-time view of local network traffic
4. Attacker Workstation – What the adversary is doing
5. Video Screen – Camera feed of plant discharge at lagoon to indicate plant activity
6. Event Log – Shows activity on water plant PLC
7. RSLogix – shows actual programming in water plant PLC
8. Event Sentry – Consolidates event logs from multiple devices
9. Threat Map – Internet threat tracking application

Figure 2.1: Observer Room Screens

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Attack Vectors and Desired Effects

A public-facing Internet Protocol (IP) address connected to the Internet is defended by a firewall that connects the Internet Service Provider (ISP) to the business network. A single physical switch (Cisco) is VLANd off from the process network. For Crit-Ex 16.2, the attack will be of two varieties:

- Brute Force – Designed to start attacking a public-facing IP.
    - The end result will be the attacker pushing through the Sonicwall (Demilitarized Zone [DMZ]), bridging the two Virtual Local Area Networks (VLAN) and then enabling a Remote-Access Trojan (RAT) of the PLC programming software, allowing the hacker to modify code without the operator seeing a change on his screens.
- Watering Hole – Operator visits an approved website that has been compromised causing a malicious payload to be delivered.
    - Following the start-up of the malicious payload, an outbound connected HTTPS connection is made on tcp/443 through the firewall.
    - At that point the attacker can initiate commands with the infected host, and a series of commands can then be run to allow full control of the machine and other interconnected systems.
    - Each of the commands below will be executed on the compromised machine (agent) making an outbound connection to the listener.

Desired effects of attacks include the following:

- By reprogramming high-service (HS) pump controls, the bad actor will be able to:
    - Stop water flow through the distribution network, causing a boil-water order to be issued, or;
    - Cycle HS pumps, causing water hammer and burst pipes.
- By reprogramming filter controls and turbidity reports, the bad actor will be able to:
    - Generate non-potable water and distribute it to the population, requiring flush and boil orders.

Exercise Scenario Background

Phase 1: "Business as Usual"

A state-sponsored terrorist group has begun a targeting campaign aimed at small utility companies, attempting to find vulnerabilities in their public-facing websites that will result in access to critical industrial control systems. The group has targeted smaller companies because of their lack of resources and ability to protect their growing IT networks. With the resources backing this particular terrorist group, it is only a matter of time before access is granted, likely without the utility companies having any notification of malicious intrusion into their network.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

During this campaign, the state-sponsored group has successfully accessed a rural water utility company's critical infrastructure network via a brute force attack passing through the DMZ. Once inside the network, the group is able to pivot laterally without detection from operational and technical controls. With such ease of movement, the group has successfully changed the code to a PLC, giving it the ability to control the water-related functions of this PLC anytime it chooses. The advantage for the terrorist group changing the code is two-fold in nature because the operator at the water company does not see any change on their HMI display. Once the process is triggered, the only way an operator would become aware of the change is after something drastic has already occurred in the distribution network.

Key Issues

- Indiana is experiencing potential water disruption that affects various water utility companies around the state.
- Utilities are not aware that a cyberattack has caused this disruption, and most are going through normal recovery operations.

Questions

The following questions are provided as suggested general subjects. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

- What initial actions would your organization take? What are your organization's first priorities?
- Who is your first call? How do you identify your critical partners for a disruption?
- Would information presented in this phase (or this stage of the attack) be shared? Who is contacted as part of the alert/notification process?
  - Local government, police, fire, emergency services, and trusted third parties?
  - State partners and/or agencies?
  - Federal partners and/or agencies?
- Are manual overrides available to allow operation of key processes?
- What are your reporting requirements? Based on your contact and alert procedures after an incident, do those match your mandated reporting requirements? Internal? Local, state, and federal levels of government?
- How do you determine when and with whom to share sensitive and/or classified information about the event, including information about proprietary systems? What concerns or considerations do you have in coordinating with or discussing your situation with external entities?
- Have you identified available resources and their specific requests channels for a water disruption?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

After Action Review Discussion Topics for Consideration

- Assess the effectiveness of the organization's incident reporting and notification process.
- Determine how and how quickly utilities communicate with interdependent facilities, emergency management and government following an attack.
- Identify when intelligence and information is shared, and with whom.
- Identify available resources and resource request channels for a water disruption.

Phase 2: "Fool Me Twice"

As the state-sponsored terrorist group campaign persists against small utility companies, it continues to find vulnerabilities that add to its overall attack package. It has already successfully changed the normal operating functions of many utility companies in the past few weeks, causing them to revert to manual operation while IT-related issues were resolved. Most of the companies are unaware that the change in functions could be attributed to a cyberattack, and those that have suspicions have failed to share their findings with other utilities. Some attack vectors previously exploited by the group have been revoked because of normal IT procedures. That may have fixed the initial intrusion, as a persistent threat always looks for another way in.

Normal processes and procedures in the daily life of utility operators can seem menial, but to an attacker they present opportunities to exploit vulnerabilities of daily operations. A website used by many utility operators in the area has been compromised by the group, and when users think they are checking local weather reports a malicious payload is dropped onto their system. From there, the group is able to capture a multitude of data, helping them develop secondary attack vectors in the chance that their initial vector is closed off. The result is the same; it gives the group complete access to pivot inside the utility network without being detected. Having that ability allows the attackers to change whatever they want without operator knowledge and repeat and/or initiate new attacks against compromised utility companies.

Key Issues

Utilities are now aware that a cyber-attack has caused this disruption.

Questions

The following questions are provided as suggested general subjects. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

- How and with whom will this information be communicated?
- Does this information change your priorities? How? How will it affect your response operations? How would a law enforcement investigation impact your current operations?
- How does the attribution of a terrorist cyberattack change your priorities and courses of action?
- What types of sensitive information/intelligence need to be communicated outside your organization, and how will that be delivered?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

- Does your organization have the resources it needs to respond to this cyberattack? How will you request more resources?
- What protective actions would you take across non-impacted systems or agencies?
  - Who is responsible for protective action decision-making?
  - How are actions coordinated across departments/agencies?
- How will you address public safety issues? With what agencies/entities will you coordinate?
- What plans, procedures, and/or agreements do you have in place to control resource distribution within and outside your jurisdiction?
- Is a Crisis Management Team identified with at least one representative from executive management? Does the team have the authority to declare the disaster and coordinate necessary recovery activities?
- Is there an Incident Response Plan and does it include a contact list and procedures for contacting necessary personnel? Is there a back-up plan if essential personnel cannot be reached?
- Does the organization have consistent contact with intelligence organizations to stay abreast of current threat Tactics, Techniques, and Procedures (TTPs)? Are changes made to security procedures based on available intelligence?
- Are written Service Level Agreements (SLA) established for all identified external dependencies? Are expectations for response times/restoration included? Are they exercised to ensure external organizations can realistically meet demands?
- Are SLAs with staff and contracted employees established to respond in emergency conditions?
- Have you identified available resources and their specific requests channels for a water disruption?

After Action Review Discussion Topics for Consideration

- Examine the effectiveness of the organizations intelligence information-sharing protocols.
- Explore what polices and/or procedures are in place to identify a cyber incident.
- Explore what policies and/or procedures are in place to mitigate and react to a cyberattack.
- Identify available resources and resource request channels for a water disruption.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Phase 3: After Action Review Discussion

After these functional group discussions, participants will engage in a facilitated After Action Review discussion in which representatives from each utility will present a synopsis of the group's actions based on the scenario presented. This discussion, which will be led and facilitated by identified representatives from Camp Atterbury-Muscatatuck, will also examine various strengths and lessons learned from the exercise, as well as future areas for improvement.

Evaluation of the exercise is based on a set of objectives developed by the Exercise Planning Team. Evaluators will be provided with the identified objectives, and players will be asked to complete exercise evaluation forms. These documents, coupled with facilitator observations and notes compiled during the After Action Review process will be used to evaluate the exercise and compile the AAR.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

SECTION 3: EXERCISE APPENDICES

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix A: Exercise Schedule – Day 1 (Groups 1, 2, and 3)

May 18, 2016

May 18, 2016 – Indiana American Water	
Time	**Activity**
0800-0820	Welcome Briefing
0820-0830	Move to Building 16
0830-1000	Phase 1 - Attack 1
1000-1130	Phase 2 – Attack 2
1130+20	Reboot exercise control system for next group
1130-1200	Wrap-up and Debrief (After Action Review)
1230-1300	FBI Command Tour
1300-1400	Tour of MUTC

May 18, 2016 – Michigan City water Department	
Time	**Activity**
1120-1140	Welcome Briefing
1140-1150	Move to Building 16
1150-1320	Phase 1 - Attack 1
1320-1450	Phase 2 – Attack 2
1450+20	Reboot exercise control system for next group
1450-1520	Wrap-up and Debrief (After Action Review)
1530-1600	FBI Command Tour
1600-1700	Tour of MUTC

May 18, 2016 – Carmel Utilities	
Time	**Activity**
1300-1320	Welcome Briefing
1320-1330	Move to FBI Command Center
1330-1400	FBI Command Tour
1400-1500	Tour of MUTC
1510-1640	Phase 1 – Attack 1
1640-1810	Phase 2 – Attack 2
1810	Reboot exercise control system (for day 2)
1810-1840	Wrap-up and Debrief (After Action Review)

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise Schedule – Day 2 (Groups 4, 5, and 6)

May 19, 2016

May 19, 2016 – Evansville Water & Sewage	
Time	**Activity**
0800-0820	Welcome Briefing
0820-0830	Move to Building 16
0830-1000	Phase 1 - Attack 1
1000-1130	Phase 2 – Attack 2
1130+20	Reboot exercise control system for next group
1130-1230	Wrap-up and Debrief (After Action Review)
1230-1300	FBI Command Tour
1300-1400	Tour of MUTC

May 19, 2016 – Citizens Water	
Time	**Activity**
1120-1140	Welcome Briefing
1140-1150	Move to Building 16
1150-1320	Phase 1 - Attack 1
1320-1450	Phase 2 – Attack 2
1450+20	Reboot exercise control system for next group
1450-1520	Wrap-up and Debrief (After Action Review)
1530-1600	FBI Command Tour
1600-1700	Tour of MUTC

May 19, 2016 – Fort Wayne Utilities	
Time	**Activity**
1300-1320	Welcome Briefing
1320-1330	Move to FBI Command Center
1330-1400	FBI Command Tour
1400-1500	Tour of MUTC
1510-1640	Phase 1 – Attack 1
1640-1810	Phase 2 – Attack 2
1810-1840	Wrap-up and Debrief (After Acton Review)

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix B: Core Capability/AWWA Practice Standards Crosswalk

Exercise OBJ 1: Protect/restore the SCADA system information and services from damage, unauthorized use, and exploitation by malicious activities

	Intel/ Info Sharing	Sit Assessment	Infrastructure Systems	Op Com	Op Coord	Cyber security	Access Control	Physical Protective Measures	Risk/Disaster Resilience Assessment	Community Resilience	Risk Management for Protection Programs & Activities	Interdiction & Disruption
Governance/ Risk Mgmt		X			X	X	X	X	X	X	X	
Business Cont/ Disaster Recovery		X	X	X	X	X			X	X		
Server/ Workstation Hardening	X					X		X	X			X
Access Control						X	X		X			X
Application Security						X	X		X			X
Encryption			X	X		X	X	X	X			X
Telecomms/ Network Sec/Arch	X		X			X	X	X	X		X	X
Physical Security of PCS Equipment						X	X	X	X			X
Service Level Agreements		X		X		X	X		X	X		
OPSEC						X	X		X		X	X
Education	X			X		X	X		X	X		X
Personnel Security						X	X		X		X	X

Most Relevant Questions:

- Does the organization implement a cyber-security awareness program that cross trains Process Control System (PCS) & IT staff on best practices for PCS cybersecurity and trains personnel on risky behaviors /threats (including social engineering)?
- Is there a formal, written Cybersecurity policy that addresses the specific operational needs of PCs, contains priorities for mission/objectives/activities, established cybersecurity roles & responsibilities for the entire workforce/3rd party stakeholders, legal requirements, and includes an information security policy?
- Does the organization have consistent contact with intelligence organizations to stay abreast of current threat Tactics, Techniques, and Procedures (TTPs)? Are changes made to security procedures based on available intelligence?
- Does the organization conduct vulnerability assessments on a regular basis?
- Does the organization maintain a PCS asset inventory?
- Are PCS Cybersecurity standards articulated/required in all procurement packages?
- Is storage encryption implemented for devices that could be stolen?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise OBJ 2: Stabilize water infrastructure functions, minimize health & safety threats, and efficiently restore and revitalize systems and services to support a viable resilient community

	Intel/ Info Sharing	Sit Asst	Infrastructure Systems	Op Com	Op Cord	Cyber security	Access Control	Physical Protective Measures	Risk/Disaster Resilience Assessment	Community Resilience	Risk Management for Protection Programs & Activities	Interdiction & Disruption
Governance /Risk Mgmt					X				X	X		
Business Cont/ Disaster Recovery		X	X		X				X	X		
Server/Workstation Hardening												
Access Control					X							
Application Security												
Encryption				X								
Telecomms /Network Sec/Arch		X		X					X	X		
Physical Security of PCS Equipment												
Service Level Agreements		X	X	X	X				X	X		
OPSEC												
Education	X	X										X
Personnel Security												

Most Relevant Questions:

- Are written Service Level Agreements (SLAs) established for all identified external dependencies? Are expectations for response times/restoration included? Are they exercised to ensure external organizations can realistically meet demands?
- Are SLAs with staff and contracted employees established to respond in emergency conditions?
- Is a Crisis Management Team identified with at least one representative from executive management? Does the team have the authority to declare the disaster and coordinate necessary recovery activities?
- Are manual overrides available to allow operation of key processes?
- Are strategies in place to provide redundancy of key system components and can they be implemented within an acceptable timeframe?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise OBJ 3: Bring awareness to the current readiness of water utilities to respond to a cyber- attack and draw out best practices for improving systems security and incident response

	Supply Chain Integrity/ Security	Logistics & Supply Chain Mgmt.	Intel/ Info Sharing	Op Com	Op Cord	Screening/ Searching/ Detection	CS	Physical Protective Measures	Risk/ Disaster Resilience Assessment	Community Resilience	Risk Management for Protection Programs & Activities	Threats/ Hazards ID	Infra-structure Systems	Sit Asst
Governance /Risk Mgmt	X				X		X		X	X	X			X
Business Cont/ Disaster Recovery	X	X		X	X		X		X	X			X	X
Server/ Workstation Hardening			X			X	X	X	X			X		
Access Control							X	X	X					
Application Security							X		X					
Encryption				X			X	X	X					
Telecomms/ Network Sec/Arch	X		X			X	X	X	X		X	X	X	
Physical Security of PCS Equipment							X	X	X					
Service Level Agreements	X	X		X			X		X	X			X	X
OPSEC	X		X				X		X		X			
Education			X	X		X	X		X	X		X		
Personnel Security						X	X		X		X			

Most Relevant Questions:

- Does the organization have consistent contact with intelligence organizations to stay abreast of current threat TTPs? Are changes made to security procedures based on available intelligence?
- Is a Crisis Management Team identified with at least one representative from executive management? Does the team have the authority to declare the disaster and coordinate necessary recovery activities?
- Is there an Incident Response Plan and does it include a contact list and procedures for contacting necessary personnel?
- Are manual overrides available to allow operation of key processes?
- Are written SLAs established for all identified external dependencies? Are expectations for response times/restoration included? Are they exercised to ensure external organizations can realistically meet demands?
- Are SLAs with staff and contracted employees established to respond in emergency conditions?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Exercise OBJ 4: Provide water utility observers with the training that empowers them for a real world emergency, identifying key decision points and decision-making

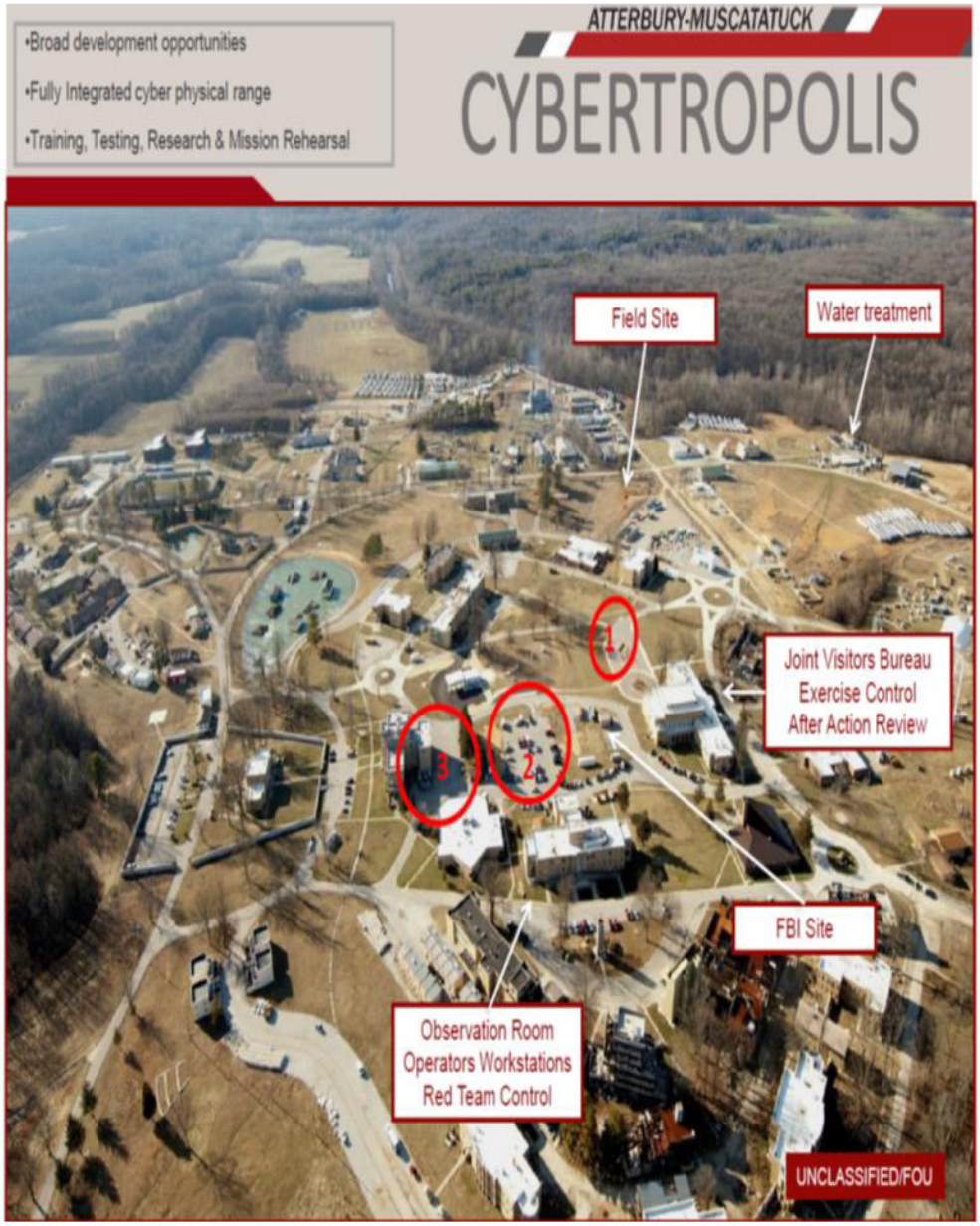
	Intel/ Info Sharing	Sit Asst	Infrastructure Systems	Op Coms	Op Cord	Cyber security	Access Control	Physical Protective Measures	Risk/Disaster Resilience Assessment	Community Resilience	Risk Management for Protection Programs & Activities	Interdiction & Disruption
Governance/ Risk Management		X				X			X	X		
Business Cont/ Disaster Recovery		X	X			X			X	X		
Server/Work station Hardening	X					X			X			
Access Control						X			X			
Application Security						X			X			
Encryption						X			X			
Telecomms/ Network Sec/Arch	X					X			X			
Physical Security of PCS Equipment						X			X			
Service Level Agreements		X	X			X			X	X		
OPSEC						X			X			
Education	X					X			X	X		
Personnel Security						X			X			

Most Relevant Questions:

- Does the organization have consistent contact with intelligence organizations to stay abreast of current threat TTPs? Are changes made to security procedures based on available intelligence?
- Are procurement policies leveraged to limit the number of external support organizations?
- Is a Crisis Management Team identified with at least one representative from executive management? Does the team have the authority to declare the disaster and coordinate necessary recovery activities?
- Are manual overrides available to allow operation of key processes?
- Are strategies in place to provide redundancy of key system components and can they be implemented within an acceptable timeframe?
- Are written SLA established for all identified external dependencies? Are expectations for response times/restoration included? Are they exercised to ensure external organizations can realistically meet demands?
- Are SLA with staff and contracted employees established to respond in emergency conditions?

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix C: Muscatatuck Urban Training Center Map & Locations



- "Lot 1" is reserved for ranking officials and specially designated VIPs.
- Players and VIP's will be asked to park in "Lot 2".
- Exercise control personnel will be asked to park in "Lot 3".

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix D: Exercise Participants

State, Local and Federal Government
Indiana Department of Homeland Security
Infragard Indiana
Indiana Office of Technology
Indiana National Guard
Indiana Utility Regulatory Commission
Indiana State Police
Indiana Information Sharing & Analysis Center (IN-ISAC)
US Department of Homeland Security
Federal Bureau of Investigation

Utilities
Carmel Utilities
Citizens Energy Group/Citizens Water
Evansville Water and Sewage
Fort Wayne Utilities
Indiana American Water
Indiana Energy Association
Michigan City Water Department

Private Sector
Cyber Leadership Alliance
Frakes Engineering
Pondurance
Rook Security

Academia
Indiana University
Purdue University

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix E: Exercise Planning Team Members

Participant	Role
David Kane	Exercise Co-Director
Jennifer de Medeiros	Exercise Co-Director
Jim McHugh	Exercise Co-Director
Participant	**Role**
Doug Rapp, CLA	Exercise Planning Team Leader
Participant	**Role**
Jennifer de Medeiros	Exercise Planning Core Team
Jim McHugh	Exercise Planning Core Team
Cliff Campbell	Exercise Planning Core Team
John Lucas	Exercise Planning Core Team
Doug Rapp	Exercise Planning Core Team
LTC Dave Skalon	Exercise Planning Core Team
MAJ Stacy Kennedy Barker	Exercise Planning Core Team
Tad Stahl	Exercise Planning Core Team
Nick Sturgeon	Exercise Planning Core Team
Andy Mapes	Exercise Planning Core Team
John Erickson	Exercise Planning Core Team
Chris Collins	Exercise Planning Core Team
Michael Taylor	Exercise Planning Core Team
JJ Thompson	Exercise Planning Core Team
Mark Vogler	Exercise Planning Core Team
Participant	**Role**
John Lucas	Technical Working Group
Chris Collins	Technical Working Group
JJ Thompson	Technical Working Group
Mark Vogler	Technical Working Group
Cliff Campbell	Technical Working Group
Michael Taylor	Technical Working Group
Landon Lewis	Technical Working Group
Tom Gorup	Technical Working Group
Toby Church	Technical Working Group
Tony Vespa	Technical Working Group
Joe Smith	Technical Working Group
Sabrina Couturier	Technical Working Group
Dan Ford	Technical Working Group
Rushabah Vyas	Technical Working Group
Participant	**Role**
John Erickson	Public Affairs
Amber Kent	Public Affairs
David Roorbach	Public Affairs
Stacy Kennedy Barker	Public Affairs
Jennifer de Medeiros	Public Affairs

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Participant	Role
Jonathan Witham	Legal
Brad Gavin	Legal
Jim Ehrenberg	Legal
Kelsey Colvin	Legal
Jeremy Comeau	Legal
Ryan Locke	Legal
Participant	**Role**
MAJ Stacy Kennedy Barker	MUTC
CAP Jonathan Rupel	MUTC
LTC Dave Skalon	MUTC
Phil Barker	MUTC
Gary Deckard	MUTC

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

SECTION 4: INFORMATIONAL APPENDICES

The following section includes background and example information related to cybersecurity threats and attacks on the power grid.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix F: Background Information

BlackEnergy Malware

BlackEnergy was first identified several years ago as a type of malware used to launch distributed denial of service attacks (DDoS) and steal information. The majority of BlackEnergy's computer coding appears designed to conduct highly sophisticated monitoring and recording of data – a tactic known as "sniffing." However, more recent versions of BlackEnergy, such as BlackEnergy3, have evolved into an advanced persistent threat (APT) tool used in significant geopolitical operations, including Russia, Poland, and most recently Ukraine.

Experts worry that versions of BlackEnergy could be programmed to damage pieces of critical infrastructure by hacking into its control system, since its complexity hints at a highly skilled team of hackers with a broad technical background. This latest version of BlackEnergy is "modular," making it much easier for hackers to quickly change how the malware works, and significantly harder for security analysts to find and root it out.

Also worrisome is the proliferation of BlackEnergy malware. The US Department of Homeland Security has already identified BlackEnergy malware deep within industrial control systems that operate critical infrastructure, and evidence is mounting that the bug has already been deployed around Europe and is "sleeping" until activated. Cybersecurity analysts say they are sure the bug will continue to spread, and that will lead to many more blackouts and "mysterious" malfunctions in national power grids, transportation, and other industrial infrastructure.

SQL Injection

SQL injection ("Improper Neutralization of Special Elements Used in an SQL Command") is at the top of the most recent CWE/SANS Top 25 Most Dangerous Software Errors list and must be taken seriously. [1] SQL injection occurs when untrusted user-supplied data is entered into a web application and that data is then used to dynamically create a SQL query to be executed by the database server.

If a web application is vulnerable to SQL injection, then an attacker has the ability to influence the SQL that is used to communicate with the database. The implications of this are considerable. Databases often contain sensitive information; therefore, an attacker could compromise confidentiality by viewing tables. An attacker may also jeopardize integrity by changing or deleting database records using SQL injection. In other words, an attacker could modify the queries to disclose, destroy, corrupt, or otherwise change the underlying data. It may even be possible to login to a web application as another user with no knowledge of the password if non-validated SQL commands are used to verify usernames and passwords. If a user's level of authorization is stored in the database it may also be changed through SQL injection allowing them more permissions then they should possess. If SQL queries are used for authentication and authorization, an attacker could alter the logic of those queries and bypass the security controls set up by the admin.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Web applications may also be vulnerable to second order SQL injection. A second order SQL injection attack occurs when user-supplied data is first stored in the database, then later retrieved and used as part of a vulnerable SQL query. This type of SQL injection vulnerability is more difficult to locate and exploit. Exploitation does not end when the database is compromised, in some cases an attacker may be able to escalate their privileges on the database server, allowing them to execute operating system commands.

Remote Access Trojans

Remote Access Trojans (RATs) provide cybercriminals with unlimited access to infected endpoints. Using the victim's access privileges, they can access and steal sensitive business and personal data – including intellectual property and personally identifiable information. While automated cyberattacks allow cybercriminals to attack browser-based access to sensitive applications, RATs are used to steal information through manual operation of the endpoint on behalf of the victim. Most Advanced Persistent Threat (APT) attacks take advantage of RAT technology for reconnaissance, bypassing strong authentication, spreading the infection, and accessing sensitive applications to exfiltrate data. RATs are commercially available (e.g. Poison Ivy, Dark Comet) and can be maliciously installed on endpoints using drive-by-download and spear phishing tactics.

Phishing

The act of tricking individuals into divulging sensitive information and using it for malicious purposes is not new. Social engineering attacks have occurred on the internet throughout its existence. Before widespread use of the internet, attackers used the telephone to pose as a trusted agent to acquire information. The term "phishing" has origins in the mid-1990s, when it was used to describe the acquisition of ISP account information. However, today the term has evolved to encompass a variety of attacks that target sensitive information.

Hackers targeting user information are able to profit from the increased adoption of online services for many day-to-day activities, including banking, retail, and email communication. Users of these services provide a target of opportunity in that they possess information of value. Along with an increase in the number of potential targets, there are three major factors that hackers have been able to take advantage of:

> **Unawareness of threat** - If users are unaware that their information is actively being targeted by hackers, they may lack the perspective needed to identify phishing threats and may not take the proper precautions when conducting online activities.
>
> **Unawareness of policy** - Phishing scams often rely on a victim's unawareness of organizational policies and procedures for dealing with suspicious email communication. Employees unaware of the policies of an organization are likely to be more susceptible to the social engineering aspect of a phishing scam, regardless of technical sophistication.
>
> **Hacker technical sophistication** - Hackers conducting phishing scams are leveraging technology that has been successfully used for activities such as spam, distributed denial of service (DDoS), and electronic surveillance. Even as organizations are becoming aware of phishing, hackers have responded with technical tricks to make phishing scams more deceptive and effective.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

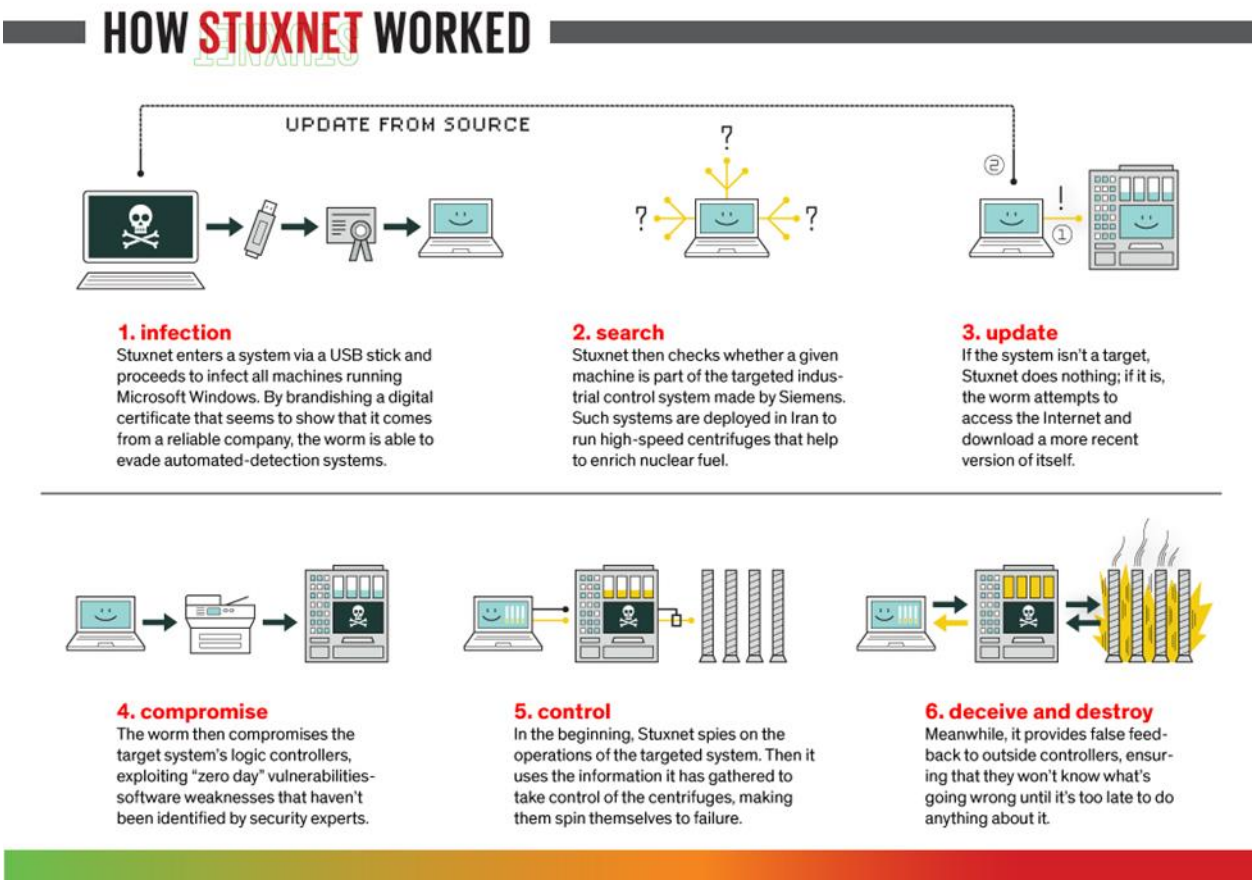
Appendix G: Case Studies

Stuxnet

One of the most famous cases involving the infection of an air-gapped system is Stuxnet, the virus/worm designed to sabotage centrifuges used at a uranium enrichment plant in Iran.

Although a computer virus relies on an unwitting victim to install it, a worm spreads on its own, often over a computer network. First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself. Then it sought out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment, such as centrifuges. Finally, it compromised the programmable logic controllers, the heart of a SCADA system. The worm's authors could thus spy on the industrial systems and even cause the fast-spinning centrifuges to tear themselves apart, unbeknownst to the human operators at the plant.

.



NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Verizon 2015 Data Breach Report

Phishing campaigns are still surprisingly effective. In the 2015 Data Breach Report, Verizon states that 23% of included recipients were found to have opened phishing messages and no less than 11% clicked on corresponding attachments. In addition, if a hacker sends out 10 emails, there is an astonishing 90% chance that at least one person will fall victim to their attack. The Verizon report also demonstrates that phishing attacks produce extremely fast results. Two of Verizon's security awareness partners sent out 150,000 phishing emails to see how many people would open the emails and what percentage would click on the links inside them. The data showed that 50% of recipients opened the email and clicked on phishing links within the first hour, with the first clicks coming in after only one minute. This report proves just how easy it is for hackers to gain access to sensitive information via simple phishing attacks. Large businesses are even more prone to these types of attacks because it can be hard to monitor the email activities of a large workforce depending on the resources each organization has.

When referring to the phishing attacks on the utility sectors, BlackEnergy used Microsoft Office documents containing malicious macros in phishing/spear-phishing attacks where the target receives an email containing an attachment with a malicious document. The document itself contains text trying to convince the victim to run the macro in the document. If victims are successfully tricked, they end up infected with BlackEnergy Lite. From there the attacker can pivot anywhere inside the network affecting critical utility controls and services.

KWC Water Plant

Hackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water, according to Verizon Security Solutions. Verizon describes the attack against the "Kemuri Water Company," a pseudonym for a real firm in an unspecified country, in this month's IT security breach report. A "hacktivist" group with ties to Syria compromised Kemuri's computers after exploiting unpatched web vulnerabilities in a payment portal that was connected to the public Internet.

The hack, which involved SQL injection and phishing - was made easier because login credentials for the operational control system were stored on the web server. The system regulated valves and ducts that controlled the flow of water and chemicals used to treat it. Verizon discovered four separate connections over a 60-day period. During these connections, the threat actors modified application settings with little apparent knowledge of how the flow control system worked. In at least two instances, they managed to manipulate the system to alter the amount of chemicals that went into the water supply and thus handicap water treatment and production capabilities so that the recovery time to replenish water supplies increased. Fortunately, based on alert functionality, KWC was able to quickly identify and reverse the chemical and flow changes, largely minimizing the impact on customers. No clear motive for the attack was found.

The hacktivists had manipulated the valves, controlling the flow of chemicals twice – though fortunately to no particular effect. It seems the activists lacked either the knowledge or the intent to do any harm. The same hack also resulted in the exposure of personal information of the utility's 2.5 million customers. There's no evidence that this has been used for fraud.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix H: Cybersecurity Glossary

Access control: The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Advanced Persistent Threat: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

Alert: A notification that a specific attack has been detected or directed at an organization's information systems.

Antivirus software: A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents – sometimes by removing or neutralizing the malicious code.

Blue Team: A group that defends an enterprise's information systems when mock attackers (i.e., the Red Team) attack, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group (i.e., the White Team).

Bot: A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under the command and control of a remote administrator.

Bot master: The controller of a botnet that, from a remote location, provides direction to the compromised computers in the botnet**.**

Computer network defense: The actions taken to defend against unauthorized activity within computer networks.

Continuity of Operations Plan: A document that sets forth procedures for the continued performance of core capabilities and critical operations during any disruption or potential disruption.

Cyber ecosystem: The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.

Cyber infrastructure: An electronic information and communications systems and services and the information contained therein.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
Denial of Service: An attack that prevents or impairs the authorized use of information system resources or services.

Distributed Denial of Service (DDoS): A denial of service technique that uses numerous systems to perform the attack simultaneously.

Encryption: The process of transforming plaintext into cipher text.

Firewall: A capability to limit network traffic between networks and/or information systems.

Hacker: An unauthorized user who attempts to or gains access to an information system.

Industrial Control System: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets.

Inside(r) threat: A person or group of persons within an organization who pose a potential risk through violating security policies.

Keylogger: Software or hardware that tracks keystrokes and keyboard events, usually surreptitiously/secretly, to monitor actions by the user of an information system.

Malicious code: Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Passive attack: An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Penetration testing: An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Phishing: A digital form of social engineering to deceive individuals into providing sensitive information.

Red Team: A group authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's cybersecurity posture.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Remote-Access Trojan: A malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program or sent as an email attachment.

Spyware: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

Supervisory Control and Data Acquisition: A generic name for a computerized system that is capable of gathering and processing data and applying operational controls to geographically dispersed assets over long distances.

Threat: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

Trojan horse: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Watering Hole Attack: a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.

White Team: A group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

Appendix I: Acronyms

AAR: After action report

APT: Advanced persistent threat

AWWA: American Water Works Association

CS: Cybersecurity

DDoS: Distributed denial of service

DHS: Department of Homeland Security

DMZ: Demilitarized Zone

EEG: Exercise evaluation guide

EMA: Emergency management agency

FOUO: For Official Use Only

HMI: Human-Machine Interface

HS: High Service

HSEEP: Homeland Security Exercise & Evaluation Program

ICS: Industrial control system

I/IS: Intelligence & Information Sharing

IDHS: Indiana Department of Homeland Security

IN-ISAC: Indiana Information Sharing & Analysis Center

INNG: Indiana National Guard

IOT: Indiana Office of Technology

IS: Information Security

IT: Information Technology

MUTC: Muscatatuck Urban Training Center

OC: Operational Coordination

OCOM: Operational Communications

PCS: Process Control System

PLC: Program Logic Controller

RAT: Remote-Access Trojan

SCADA: Supervisory Control & Data Acquisition

EXPLAN: Exercise Plan

TTPs: Tactics, Techniques, and Procedures

USB: Universal Serial Bus

VLAN: Virtual Local Area Network

NOTICE: Pursuant to Ind. Code 5-14-3, this document discusses general security measures associated with infrastructure and was developed as an intra-agency or interagency advisory or deliberative material and is an expression of opinion or are of a speculative nature, and was communicated for the purpose of decision making.

National Governors Association (NGA)
Workshop Cyber Toolkit Materials

August 2018

August 23: Cybersecurity Risk Toolkit

- Chetrice Mosley Presents Indiana Cybersecurity Scorecard
    - Changing the culture of cybersecurity
    - We could not find risk assessments that were basic enough and non-IT
    - Scorecard can apply to any entity (risk assessment in the toolkit is more operational and specific to emergency managers)
- Carlos Garcia, IU Emergency Management and Joe Romero – IU Health Presentation
    - We want emergency managers to understand the cyber threat and know how to respond pre-disaster, during disaster, and post-disaster
    - We need mitigation
    - We need preparedness—planning, training, exercise
    - We need response
    - New threat environment
        - Emergency managers simply do not have enough background to even ask the right questions on cybersecurity
        - Emergency managers tend to be reluctant to admit they do not know something, or admit they need help
        - The assessment models are just as confusing as the problem
    - Goal
        - Treat cyber risk as every other hazard
        - Convincing someone with no IT background to treat this as every other hazard
            - Assess the situation (risk assessment tool)
            - Plan (incident planning template)
            - Train and exercise (guides)
        - Key features of toolkit
            - Align NIST and FEMA/USDHS guidance
            - Preparedness Cycle model
            - Non-technical target audience
            - Ease of use
        - Risk assessment methodology
            - Incorporates NIST 800-30, CPRI, CARVER models
            - Risk measures: vulnerability, threat, impact recovery, preparedness
                - RISK = (vuln + threat + impact) – (recovery + preparedness)
                - We did not factor in probability or likelihood, assuming that the person would not know
            - User-friendly interface, easy to understand questions (turbo tax for cyber)
            - Specific to adversarial threats, most common attacks
            - Assesses internal risk based on self-reporting
        - Question: Are you going to compare entities that fill out the risk assessment?
            - Joe: No, it will be focused on the local government entity alone
- Speaker presentations

- Matt Barrett, NIST
    - The language of the CF closely aligns with the disaster management mentality of pro, during, and post-incident
    - IPDRR → 22 categories → 98 subcategories ; the value proposition is around communication and standardization—you can focus on whichever level of abstraction you need
    - You have to understand the technical ramifications of non-technical relationships
- Olga Livingston, USDHS
    - The CSF is very useful, but it does not touch on quantification of risk
    - DHS already provides assessments that range from strategic to very tactical, technical assessments
        - Cyber risk resilience review—already touches on some of the questions you already have in the risk scorecard
        - External dependency analysis
        - Cyber infrastructure survey
        - Cyber Hygiene
        - Risk and vulnerability assessment
        - More technical ones
        - Recommendation: Identify ONE core system that is critical for your business function, fix that one, then go to the next. Do not try to do everything at the same time.
    - Quantification of risk
        - ROI
            - Need to communicate loss
            - How are tools going to help you reduce the loss
        - You need more than a heatmap, you need to communicate the benefit of the cybersecurity investment, and that will allow you to explain investment to someone who might rather spend the money on a fire truck
    - DHS needs much better data to figure out the average cost of a cyber incident
        - One dataset from insurers says
            - Average is about $400,000
            - Median is $50,000
        - Other datasets say something completely different
    - Note that you need to introduce uncertainty into analysis, and pure ranking does not capture that
    - You need to form a partnership with your universities, look at students for capstones to help you solve these problems
- Doug Hormann, Raytheon
    - Risk analysis
    - First we identify critical elements in the system
    - Probability derives from

        - Accessibility
        - Exploitability (pairings of threats and vulnerabilities)
        - Capability of adversaries (threat analysis)
    - Indiana has to think about information sharing—how are emergency managers going to share information about the threats
    - Explaining what categories actually mean is critical
    - Key question: how are emergency managers going to deal with vulnerabilities that they do identify?
- Amanda Joyce, Argonne National Laboratory
    - Identifying the key people in the organizations who can actually answer the questions are often not the same person, and figuring out who can answer these assessment questions is the first priority
    - We will never reduce risk to zero
    - CPRI: this is what DHS uses in their cyber infrastructure survey tool, based on a comparability model because it lets you know where you stand in comparison to others, so then you can ask the people who are doing better, how they do it
    - We usually do not have visibility into all of our assets
    - How can you define intangible risk? You cannot necessarily quantify all risk, such as political risk for local officials
- Andrea LeStarge, Deloitte
    - Convergence of physical and cybersecurity to understand overall risk
    - Deloitte worked with another state on something very similar to what is happening in Indiana
    - Leverage threat liaison officers to get you connected to cyber liaison officers, because they are the ones who can help you fill out the tool you are designing
    - Lots of duplication across the response enterprise, so we looked at all the functions, and we had an entire matrix that went through each of the IPDRR
    - Information sharing is critical, so you need to adapt your SAR program to cybersecurity
    - We had a governor's executive order stemming from the President's EO, saying this state will have a response plan, we will disseminate a questionnaire to "open the door," then allowing the CLOs and TLOs to undertake more detailed assessments, we then created a tactical operations plan
- Questions
    - How do you incorporate human behavior?
        - It falls under the PROTECT component for training.
        - System protection, intrusion detection, adversary analysis—there is a human component in all of that; but you cannot fix stupid, so what are the administrative, procedural, and technical controls that you can implement that assumes humans will make the mistake
        - This is also why training and exercising is so important, because it allows you to assess whether behavior is actually changing

        - The NICE Framework is certainly relevant when it comes to training and behavior, because it does touch on behavior and intangible properties of behavior
        - It can be easier to measure behavior when you get more tactical, e.g., phishing
        - From an emergency management perspective, attribution is not necessarily possible, which is why information sharing is so important
    - Risk Assessment Tool Presentation
        - Key questions
            - Are we sure they will be able to answer all these questions?
            - Does the tool conflate risk assessment for the emergency manager versus risk assessment for the entire county?
        - Vulnerability
            - Critical infrastructure: need to discuss this piece of the vulnerability assessment
                - Initial thought was to include those that counties would have authority to manage
                - Does it need to include more sectors?
                - Does it need to include non-critical infrastructure?
                - Does it make sense to start with just the emergency managers, and then that becomes the conversation starter with the critical infrastructure companies—you cannot make this too big
        - Threats: methods of attack generated automatically
            - Who is the "we" in "we are vulnerable to these threats?" Are the attack vectors those that apply to the emergency manager's organization, or vectors that apply to all organizations under their potential purview?
        - Impact: criticality and harm
        - Recovery
            - How do you define normal operations?
        - Preparedness
        - Scoring
            - Based on NIST 800-30
        - Heat map displaying most serious problems

<u>Facilitation</u>

- Who is the audience?
    - District coordinators
    - Emergency management directors
    - County elected officials
        - Basic education level in some cases
    - County emergency managers
        - They have a large workload, so we need to make the assessment simple
    - This could be delegated to other audiences

- Reason for focusing strictly on emergency manager is because they are the focal point, the central point of coordination for law enforcement, EMS, and others, and they will have the path to success
- Purpose of assessment
    - Educate the center of the storm
    - Provide information to educate others
    - Start conversations with local practitioners/subject matter experts
    - Understand the threat to appropriately mitigate
    - Integrate cyber into all-hazards approach
    - Demystify cybersecurity
    - Decision aid to inform action
    - Know what risks they accept
        - **Either define it, add probability, or eliminate this**
    - Convene cross-sector representatives
    - Inward facing preparedness
    - Intelligence gathering
    - Ultimately, this is looking inward, within the emergency management agency

- This is meant to generate the conversation with those who own the infrastructure
- None of this is weighted yet; but it could be weighted based on the criticality of its impact
- How do you figure out which needs the most help
- What is the so what? What happens afterwards?
    - This moves to the plan factor
    - What is the state going to do next?
        - Inform the state of where to put their money to assist folks
- Maybe it is better to look at this as this as a survey to open the door, and then we do a real, in-depth assessment
- The action this is supposed to create is to create a response plan; to kick start the preparedness process
- Have to assess how the agencies can protect themselves, before they can support everyone else (putting their oxygen mask on first)
- What is the outcome you are trying to change?
    - Creating an IRP
    - Exercising IRP

Pros	**Cons/Improvements**
It is a clear process and feedback	Need to define terminology: put it in simple terms. E.g. ransomware is extortion Identify/define the jargon words
Hover-over feature is good	Does not delineate intent or capabilities of attackers
Turbo Tax phrase is useful	Does not address lifecycle

	Get rid of overall score because it will make people panic or misinterpret their actual risk. Make sure to call out the red areas, and not aggregate it with the green, so you can see what the true negative impact is. Need to change the mindset that just because you have an 80/100 score, that is not good enough. Don't want to lull people into a false sense of security
Self-assessment	Set a risk tolerance, perhaps
	No weighting of CI
	Shouldn't put CI at the same level as the other Infrastructures, because the latter are all dependencies on CI
	Need to be careful of what people's motives are when they do self-assessments
	Need to describe the threshold for what is "yes" or "no" when selecting an option
	Ends up treating all CI as the same
	Lack of what next
	Does not address the probability of the threat occurring; realistically, it would be useless/impossible
	No human factor
	Maybe we look at this as a survey to open the door, and then perform a real, in-depth assessment. If you call it an assessment, then people will not want to score low. But survey is more benign
	Pushing a lot of terms, and the cyber concept in general, without any context/training
	Is IT technology equipment too narrow? How do you define it
	Need to show that all hazards can effect cybersecurity (heat wave can impact technology)
	Need to include mutual aid and how it applies to cyber

<u>Vulnerability</u>

What is missing?

- Government facilities
  - Need to define this
  - Need to define emergency services
- Where are they key nodes for where communications come into the county?
- Network infrastructure needs to include security equipment
- How do you quantify the human vulnerability?
- Policies to operations

Threats

- Need to simplify methods
- Differentiate between techniques and methods; ensure that methods of attacks and their payloads are correct and defined
- Consider using anecdotes with each threat type and the risk associated with that

Impact

- The impact to the CI never changes; what matters is how you reduce the risk to avoid that impact
- This is business impact analysis

Recovery

- Recovery is restoration of services
- Need to include short term and long-term recovery
- Need to translate/crosswalk terminology
- Adjust this so it includes long term outage of a service, perhaps
- DR Recovery strategy without accounting for attacks
- Need to ask if they have a DR strategy and then ask specifics

Preparedness

- Prevention, detection, mitigation under preparedness
    - Information security (password management, firewalls, cyber hygiene, what are you doing to keep data safe?)
    - Training and education (also includes cyber hygiene)
- Need to simplify the answers. Want to know the readiness posture
    - Example: do you have a written information security plan? Needs to be concise
        - Do you hold/or participate in exercise and drills
- Need to have the hover box be very detailed

APPENDIX D.15

LEGAL & INSURANCE WORKING GROUP

LEGAL AND INSURANCE WORKING GROUP STRATEGIC PLAN

Chair: Curtis Hill | Co-Chair: Stephen Reynolds

September 2018
Indiana Executive Council on Cybersecurity

Legal and Insurance Working Group Plan

Contents

Committee Members **4**
Introduction **6**
Executive Summary **8**
Research **10**
Deliverable: Insurance Guide **18**
General Information 18
Implementation Plan 19
Evaluation Methodology 24
Deliverable: Policy Review **26**
General Information 26
Implementation Plan 27
Evaluation Methodology 31
Deliverable: Cyber Insurance Survey **33**
General Information 33
Implementation Plan 34
Evaluation Methodology 38
Supporting Documentation **40**
Cyber and Technology Insurance Guide Version 1 41
Survey of Cyber Laws 429

Committee Members

Committee Members

Name	Organization	Working Group Position	IECC Membership Type
Curtis Hill	Indiana Attorney General	Chair	Voting
Stephen Reynolds	Ice Miller	Co-Chair	Advisory
Douglas Swetnam	Indiana Attorney General	Chair Proxy	Voting Proxy
Jan Campbell	Leeuw Oberlies & Campbell, P.C.	Full Time	Advisory
Jim Ehrenberg	Indiana Office of Technology	Full Time	Advisory
George Lyle	Purdue University	As Needed	Advisory
Frank Nevers	Eskenazi Health	As Needed	Advisory
William Russell	Cummins, Inc	Full Time	Advisory
Mark Swearingen	Hall, Render, Killian, Heath & Lyman, P.C.	Full Time	Advisory
Amy Beard	Indiana Department of Insurance	Full Time	Advisory
Adam Krupp	Indiana Department of Revenue	As Needed	Voting
Brian Mcginnis	Barnes & Thornburg	Full Time	Advisory
Scott Miller	Citizens Energy Group	As Needed	Advisory
Leon Ravenna	KAR Auction Services	Full Time	Advisory
Nicholas Reuhs	Ice Miller	Full Time	Advisory
Alejandro Valle	Citizens Energy Group	Full Time	Advisory
Todd Vare	Barnes & Thornburg	Full Time	Advisory
Von Welch	Indiana University	As Needed	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - General Liability insurance exclusions
  - Cybersecurity-related insurance products
  - National Association of Insurance Commissioners Standards
  - OHIO Safe Harbor Bill
  - New Jersey Cybersecurity Bill
  - New York (NY) Financial Services
  - New York Shield law
  - United Kingdom (UK) Cybersecurity Policy
  - Wisconsin (WI) Broadband Bill
  - Indiana Office of Technology (IOT) Consumer TIPS ACT of 2017
  - Washington (WA) Biometric Bill
  - Small Business Cybersecurity Act 2017
  - New York Shield Law & NY Financial Services
  - Virginia HB 679 personal information
  - Verizon 2017 Data Breach report
  - Washington (HB 1493)
  - Cybersecurity insurance presentation by CHUBB
  - Cybersecurity insurance presentation by Travelers
  - Cybersecurity insurance presentation by Evolve MGA
  - State UDAP statutes, state Personal Information Protection Acts, state Data Breach of Security Acts for all 50 states plus District of Columbia
  - Federal statutes
  - General Data Protection Regulation (GDPR)

- **Research Findings**
  - Cybersecurity incidents are generally excluded from General Liability coverage.
  - A variety of companies are currently competing to serve the burgeoning market for insurance products covering cybersecurity-related services and risks.
  - There is no consistency between the cybersecurity policies currently offered in the marketplace.
  - There are approximately 12 different types of cybersecurity-related coverages.
  - There is no central collection of applicable state, federal and international laws with which Indiana businesses and local governments comply.

- **Working Group Deliverables**
  - Insurance Guide defining the different types of service and coverage
  - Relevant statutes and regulations
  - Cyber Insurance Survey

Additional Notes
  - None at this time.

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. **Department of Revenue (DOR)**
        i. Provided security awareness training to all full-time employees (FTEs), contractors, temps, and vendors at on-boarding and annually thereafter. This training apprises employees of the data they must protect, and the methods by which they must be protected.
        ii. Led a Continuity of Operations plan exercise in 2014—next one projected for 2018
        iii. Trained and exercised the DOR Incident Response team and plan annually
        iv. Sent periodic e-mails and published articles in agency publications apprising all DOR employees of security issues and best security practices
        v. Sent e-mails to all DOR employees apprising them of urgent real-world security issues, and how to address them (e.g., phishing messages and phone-based social engineering attacks)
    b. **Cummins**
        i. Cummins has undertaken a multi-year effort to raise the level of cybersecurity preparedness within the company. Among the investments is a 300% increase in the number of employees working on cybersecurity and a commensurate increase in budget. We have adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework on which to base our cybersecurity programs. We have initiated an employee awareness program with regular communications and annual events during Cybersecurity Awareness Month (October). We have partnered with Ivy Tech to provide cybersecurity students hands-on experience within Cummins cybersecurity operations center in conjunction with their classroom studies in cybersecurity. This has resulted in several hires of local students upon graduation and the program now includes students from Franklin University and IUPUI/IUPUC.
    c. **Gregory Appel**
        i. Law firms, insurance brokers, and insurance carriers semi-frequently hold client (public) educational sessions geared toward clients/insureds to better grasp the exposure, threat, responsibility, and legal/insurance protection for privacy and network security liability. These sessions are generally offered from a knowledge leadership perspective, but because of their nature can be geared to an entry level of understanding of cyber liability concerns. Certain industries, such as healthcare, have moved beyond a 101 level of education/training because of their risk and regulatory environment. Many risk-oriented firms offer tabletop breach exercise simulations to test and evaluate a client/insured's incident response program's communication effectiveness.

d. **Indiana Office of Technology (IOT)**
    i. The Indiana Office of Technology instituted a computer-based cybersecurity training program that is intended to make State employees aware of common types of cyber threats and the value of basic cyber hygiene. The name of the product that was used in 2017 is Security Mentor. We also instituted a phishing simulation. Essentially, we sent spam emails to state employees with links in them. Employees who clicked on the links where directed to a webpage which explained that they had been phished and that they would be enrolled in a phishing prevention training program.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. **DOR**
        i. External threats (State and non-state cyber actors, cybercriminals, cyberterrorists, etc.)
        ii. Malicious insiders
        iii. Employees who fall for social engineering schemes
        iv. Servers containing sensitive data that reside outside of the state's protected zone (PZ)
    b. **Gregory Appel**
        i. Insurance industry statistics point to healthcare, financial and retail sectors as having the most severity. While main street, mom n' pop, and small business account for the frequency comprising approximately two-third of breaches.
    c. **Cummins**
        i. Skill gaps for employees in general related to cybersecurity and safe use of computing and network resources. In addition, as a manufacturing company, we rely on a number of legacy systems in our manufacturing processes which are difficult to patch and maintain, retiring these systems is a priority.
    d. **IOT**
        i. There are approximately 40K state employees. There are multiple layers to our cybersecurity safeguards. That said, in theory, a malicious actor could gain access to our systems if just one of those 40K employees makes a mistake. Another challenge that we have is keeping up with software updates and patches.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. **DOR**
        i. Funding and manpower to support security assessments and implementation of security enhancements
    b. **Gregory Appel**
        i. Understanding of their legal and regulatory responsibilities for privacy and network security liability and how to best structure an insurance program to work with and support a meaningful incident response plan (IRP).

c. **Cummins**
    i. Our greatest challenges are in synchronization of global operations in a complex regulatory environment. Differing requirements and technology limitations make the operation of a global cybersecurity infrastructure very complex and difficult.
d. **IOT**
    i. Our biggest need is in manpower. There are just 11 employees on the IOT Security Team.

4. **What federal, state, or local cyber regulations is your area beholden to currently**?
    a. **DOR**
        i. Internal Revenue Service (IRS) Publication 1075
        ii. NIST Special Publication 800-53: Using Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) for detailed security assessments
        iii. Indiana Code and policies
        iv. IOT policies and standards
        v. DOR policies and procedures
    b. **Cummins**
        i. Sarbanes Oxley, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Defense Federal Acquisition Regulation Supplement (DFARS), China Cybersecurity Law, Data residency rules in India and European Union, GDPR.
        ii. US China Commission studies on cyber capabilities of the Peoples Liberation Army.
    c. **Gregory Appel**
        i. All of them. With approximately 48 different State Breach Statutes and a potential myriad of Federal and International regulatory frameworks, educating a client on how to navigate them from a legal or insurance perspective is at best challenging.
    d. **IOT**
        i. We maintain various types of confidential information for state agencies; including personal health information, personally identifiable information, data from the Social Security Administration, federal tax information, etc. We are required to abide by HIPAA, IRS Publication 1075, and other state and federal laws calling for the protection of such information.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. **IOT**
        i. The Information Security Research and Education (INSuRE) program researches and seeks solutions to hard security problems. INSuRE members are the US Intelligence Community, US National Laboratories, US universities and colleges which include Purdue, and State government organizations such as IOT.

b. **Gregory & Appel**
    i. Most Insurance carriers offering cyber liability (and technology errors & omissions) have pre-packaged claim scenarios, actual paid claim losses with detail scrubbed of the names of the innocent. Indiana Security & Privacy Network (INSPN) for example regularly highlights recent breaches during its quarterly update.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    i. [No response]

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. All other state departments of revenue/taxation that receive Federal Tax Information (FTI) are required by IRS to provide:
        i. Security awareness training for all employees
        ii. Role-based training to personnel based on assigned security roles and responsibilities
        iii. Contingency training for personnel responsible for recovering backup copies of FTI
        iv. Incident response training to personnel responsible for handling and reporting security events.
    b. Other Attorney General offices enforce their state data privacy, security, and data breach laws.

8. **What does success look like for your area in one year, three years, and five years?**
    a. **DOR**
        i. Year 1
            1. Conduct security assessments
            2. Implement security controls, address severe and significant vulnerabilities and threats
        i. Year 3
            1. DOR, its vendors, partners, and e-filing tax community comply with DOR security requirements
            2. Work towards the following goals
                a. All sensitive DOR servers reside in the state's PZ
                b. DOR servers reside within appropriate network segments
                c. All sensitive DOR data within the state network is encrypted at rest and in motion
                d. DOR users have least privileged access
                e. Security patching is done immediately
                f. Continuity of Operations (COOP) and Disaster Recovery (DR) plans are developed, appropriately resourced, and successfully tested
        i. Year 5: Achieve the following goals
            1. All sensitive DOR servers reside in the state's PZ

2. DOR servers reside within appropriate network segment
3. All sensitive DOR data within the state network is encrypted at rest and in motion
4. DOR users have least privileged access
5. Security patching is done immediately
6. COOP and DR plans are developed, appropriately resourced, and successfully tested

b. **Cummins**
   i. A modernized IT infrastructure, operated and maintained by a trained IT and cybersecurity workforce that is able to quickly detect and respond to malicious activity to maintain business operations.

c. **IOT**
   i. In the short term, we would like to develop a formal cybersecurity incident response plan that will allow us to respond to incidents timely, effectively, and appropriately. In the long run, we would generally like to increase our cybersecurity protections and preparedness.

d. **Gregory & Appel**
   i. A public better informed about their responsibilities in a breach and what or how a cyber liability product can risk transfer the monetary cost of implementing an IRP. More insureds purchase cyber today than three years ago and more will purchase it three years from now than purchase today and at higher limits. It very much should become a part of most Commercial Insured Risk Transfer/Insurance program.

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

a. **DOR**
   i. The public should be apprised that DOR continuously implements tools and processes to bolster cybersecurity to protect their information, which may appear inconvenient to them. For example, we may require taxpayers logging into our applications to increase the length and complexity of their passwords.

b. **Cummins**
   i. Better user training beginning in K-12 so we have a well-informed workforce able to safely operate their IT resources.

c. **Gregory & Appel**
   i. There should be more industry-focused cyber liability workshops or tabletop breach exercises geared towards educating a particular industry group about their key exposures, the cost, and how to think about cyber insurance effectively.

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. **DOR**
   i. Total DOR Workforce as of December 2017: 751. 659 FTEs and 92 contractors.
   ii. Total DOR Cybersecurity Staff: 6

iii. Total DOR Cybersecurity Staff shortfall: 0

b. **Cummins**
   i. We have approximately 1000 total IT employees within Cummins. Cybersecurity is currently at 45 employees and we have 2-4 vacancies at any given time.

c. **Gregory & Appel**
   i. Most of the insurance carrier resources dedicated to cyber liability reside outside of Indiana with Chicago comprising the most concentrated hub of underwriting talent. Many larger insurance brokers purport to have experienced cyber brokers on staff or available (any licensed insurance agent can sell a cyber policy, but not all of them are comfortable with the nuances). Most law firms in the city have a cyber practice.

d. **IOT**
   i. There are approximately 40K state employees. There are approximately 440 IOT employees and contractors. The IOT Security Team has 11 employees. Other agencies have security personnel as well. However, their focus is not entirely on security.

11. What do we need to do to attract cyber companies to Indiana?

a. There is already some very good IT security and forensics firms such as Pondurance and Rook located in Indiana.
b. Attracting cyber talent is what is needed.

12. What are your communication protocols in a cyber emergency?

a. **DOR**
   i. DOR employee, IOT, or anyone else identifies and reports suspicious activities to DOR Security Team
   ii. DOR Security Team assesses and analyzes the situation, and determines if there is an emergency
   iii. DOR Security Team, upon DOR Chief Information Officer (CIO) approval, takes immediate action as necessary to stop the perpetuation of damage
   iv. DOR Security Team develops multiple courses of action (COA) to address remaining security concerns and to recover from the event, then presents them to other members of the DOR Incident Response Team comprising DOR Chief Operating Officer, DOR Chief Information Officer, DOR Inspector General, DOR Legal Team, DOR Communications Team, and IOT Chief Information Security Officer
   v. DOR Incident Response Team decides on a single course of action
   vi. DOR Incident Response Team briefs DOR Commissioner on the situation, actions taken, and proposed COA
   vii. DOR Commissioner approves COA
   viii. DOR Incident Response Team works with IOT to execute the approved COA

b. **Cummins**
   i. We manage crisis communication centrally with a cross-functional working group made up of decision makers from legal, finance, IT, business

operations, HR and Global Security. Cummins does not publicly discuss details of malicious activity unless required by regulation or law.

c. **IOT**
    i. Notice of a cyber event typically comes to the Security Operations Center. The SOC handles the situation if it is a relatively minor event – e.g., a virus protection situation. If the situation requires a higher level of expertise, such as a spam email with malicious links or attachments to multiple state employees, it is escalated to the IOT Security Team which considers if other teams inside and outside of IOT should be alerted. If the IOT Security Team determines that it cannot contain the event on its own, it contacts the IOT Chief Information Security Officer (CISO) and CIO.

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. Defense-in-depth: an information assurance concept in which multiple layers of security controls are placed throughout an information technology system
b. Initial and annual security awareness training
c. Phishing testing

Deliverable: Insurance Guide

Deliverable: Insurance Guide

General Information

1. **What is the deliverable?**
    a. Document describing various types of coverages available in existing cybersecurity insurance policies.

2. **What is the status of this deliverable?**
    a. Version 1 Complete 100%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns.**
   See Executive Order 17-11 for further context.
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. A guide for Indiana residents describing the different types of coverages and services available in "cybersecurity policies"

6. **What metric or measurement will be used to define success?**
    a. Completed documents made publicly available through state websites.

7. **What year will the deliverable be completed?**
    a. Initial version was completed in 2018. Subsequent versions will be released yearly.

8. **Who or what entities will benefit from the deliverable?**
    a. All Indiana businesses.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Strategic resource and Public Awareness Training

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. We are meeting with the leading cybersecurity insurance companies to gather the different coverages and services offered under a cyber risk policy.

12. **Who should be main lead of this deliverable?**
    Reid Putnam (with assistance from Nick Reuhs and Jan Campbell)

13. **What are the expected challenges to completing this deliverable?**
    a. Cyber risk and liability insurance is a new and fast-changing marketplace, so the information will likely change each year for the next five to ten years.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. This will require periodic updates, at least annually.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Meeting and discussion with representatives from leading cybersecurity policy providers	Reid Putnam	100%	Completed May 2018	
Publicize availability of Insurance and resources	Needs to be assigned to communication committee	0%	December 2018	
Conduct survey of businesses for insurance coverage and cybersecurity insurance coverage	Cybersecurity Council (perhaps working with Secretary of State to be done with annual corporate reports)	0%	2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
¼ FTE	¼ FTE	cybersecurity insurance broker	Cybersecurity Council office	Indiana General Assembly appropriation	
¼ FTE	1/16 FTE	Communications	Cybersecurity Council office	Indiana General Assembly	
¼ FTE	¼ FTE	Survey	Cybersecurity Council office	Indiana General Assembly	Secretary of State should be involved

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Website space	Making documents available for review or download	May be within scope of current IN website maintenance	unknown	Cybersecurity Council office	Indiana Legislature	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. By publishing details on types of services and insurance coverages commercially available, Indiana businesses and local governments will increase awareness and understanding of cyber risks and the products available to manage those risks.
b. By increasing the number of businesses protected against cybersecurity loss, Indiana's economy will be more resilient in the face of increasing cyber threats.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. It has been estimated up to 60% of small and medium-sized businesses fail within 6 months of a cybersecurity attack. By encouraging small and medium-sized businesses to protect against cybersecurity risk, Indiana companies and local governments will be better protected.

19. What is the risk or cost of not completing this deliverable?

a. Up to 60% of small and medium-sized businesses fail within 6 months of a cybersecurity attack, and the risk of being targeted by an attack is rising exponentially. Indiana's economy could be damaged as the result of cyber attacks against Indiana businesses and local government.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completed list of currently available cybersecurity coverages and services.
b. There is no current survey of Indiana businesses on this subject. Cybersecurity council could work with 1) Indiana Chamber of Commerce, or 2) Secretary of State's office to conduct a survey of Indiana businesses, and use the increase of businesses covered by cybersecurity policies as a measure of success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No
b. **If Yes, please list states/jurisdictions**
   i. Other states or jurisdictions are likely analyzing similar information, but we are not currently aware of concrete examples.
   ii. We are not aware of initiatives in other states.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No
b. **If Yes, please list states/jurisdictions**
   i. We are not aware of similar initiatives in other states, but cybersecurity is a hot topic and there has been a flurry of activity at the state level.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability of committee members.
b. Scheduling conflicts among committee members.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
   i. Making insurance coverage and specifically cybersecurity insurance coverage part of a corporation's annual or semi-annual filing with Secretary of State would require legislative and administrative change.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. The list of applicable laws will require continual updating.
b. The types of coverages available under cybersecurity insurance policies are changing as cybersecurity risks change and will require continuous updating.
c. Surveys of businesses will require annual surveys or coordination with Indiana Chamber of Commerce or Secretary of State.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Insurance policy coverages:
   i. American International Group (AIG)
   ii. Chubb
   iii. Travelers Insurance
   iv. CNA insurance

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All sectors

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All stakeholders would benefit from this information.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Indiana cybersecurity office could coordinate with Chris Profitt, Director of Communications for Office of Indiana Attorney General, and Mary Allen, Director of Outreach for Office of Indiana Attorney General.
b. Indiana Chamber of Commerce could help promote.

Evaluation Methodology

Objective 1: IECC Legal and Insurance Working Group develop a Cyber Insurance Guide to be provided to government and businesses by September 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Policy Review

Deliverable: Policy Review

General Information

1. **What is the deliverable?**
   a. List of cybersecurity laws and regulations for Indiana businesses and residents

2. **What is the status of this deliverable?**
   a. Version 1 is 100% complete.

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Companies, local governments and individuals will be better able to comply with relevant laws.

6. **What metric or measurement will be used to define success?**
   a. A completed document that captures all current, applicable laws.

7. **What year will the deliverable be completed?**
   a. Initial version was completed in 2018. Subsequent versions will be released as needed.

8. **Who or what entities will benefit from the deliverable?**
    a. The document will educate Indiana businesses and local government about their responsibilities under existing cyber laws.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Public Awareness and Training.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Attorney General offices across the United States and data privacy and security attorneys on Legal and Insurance Working Group.

12. **Who should be main lead of this deliverable?**
    a. Doug Swetnam/Stephen Reynolds

13. **What are the expected challenges to completing this deliverable?**
    a. Availability of committee members.
    b. Scheduling committee members.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Cybersecurity laws are rapidly changing and new lists will need to be compiled at least annually, if not more frequently.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review and revise list of laws applicable to Indiana businesses and residents under current landscape	Doug Swetnam/Stephen Reynolds	Version 1 100% complete	August 2018	Federal and State legislation should be monitored for changes in existing laws.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
¼ FTE	¼ FTE	Legal – legislative – Track legislative updates to cyber laws in all jurisdictions affecting IN	Cybersecurity Council office or Indiana Attorney General	Indiana General Assembly appropriation	
¼ FTE	1/16 FTE	Communications	Cybersecurity Council office	Indiana General Assembly	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Website space	Making documents available for review or download	May be within scope of current IN website maintenance	unknown	Cybersecurity Council office	Indiana legislature	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Businesses and local governments will have a legal reference to identify the current patchwork of cybersecurity laws, regulations and requirements.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. It has been estimated up to 60% of small and medium sized businesses fail within 6 months of a cybersecurity attack. By making companies more aware of the legal requirements expected of them, and the potential penalties and liability for non-compliance, they will be better motivated to plan and prepare for a cyber emergency.

19. What is the risk or cost of not completing this deliverable?

a. Up to 60% of small and medium sized businesses fail within 6 months of a cybersecurity attack, and the risk of being targeted by an attack is rising exponentially. Indiana's economy could be damaged as the result of cyber attacks against Indiana businesses who are not prepared to respond to an incident.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Version 1 Survey of Cybersecurity laws and regulations completed.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No
b. **If Yes, please list states/jurisdictions**
   i. Other states or jurisdictions are likely looking at these statistics, but we are not currently aware of concrete examples.
   ii. We are not aware of initiatives in other states, but there may be.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. There is a possibility other states have comparable initiatives, though we are not aware of any at this time.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability of legal resources to review and verify applicable laws and regulation.
b. With the fast pace of cybersecurity rules and regulations over the past several years it is possible to omit some.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. The list of applicable laws will require continual updating.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Applicable laws – Legal and Insurance working group

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All sectors

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All stakeholders would benefit from this information.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Indiana cybersecurity office could coordinate with Office of Indiana Attorney General communications.

Evaluation Methodology

Objective 1: Legal and Insurance Working Group develop a list of cyber laws applicable to Indiana businesses and residents under the current landscape by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Insurance Survey

Deliverable: Cyber Insurance Survey

General Information

1. **What is the deliverable?**
    a. Survey of Indiana businesses who have cybersecurity insurance coverage.

2. **What is the status of this deliverable?**
    a. Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☒ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☒ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The initial objective is to create a baseline measurement of cybersecurity risk management analyses undertaken by Indiana businesses.

6. **What metric or measurement will be used to define success?**
    a. A steadily increasing number of Indiana businesses who have gone through a process to assess their cybersecurity risks and make an informed business decision as a result of that review. (Whether they choose to insure, or not.)

7. **What year will the deliverable be completed?**
    a. Annually starting 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Individual Indiana businesses will benefit from making informed cyber risk assessments, and the Indiana economy as a whole will benefit by being better prepared for cyber risks.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. The Indiana Department of Insurance gathers annual information on admitted carriers, but we do not believe any entity is currently conducting the survey we are suggesting.

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Policy working group and possibly Strategic Resources working group.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Secretary of State

12. **Who should be main lead of this deliverable?**
    Cybersecurity Council office

13. **What are the expected challenges to completing this deliverable?**
    a. No Response

Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing surveys (annually)

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Conduct a survey of businesses for insurance coverage and cybersecurity insurance coverage.	Cybersecurity Council (perhaps working with Secretary of State to be done with annual corporate reports)	0%	December 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
¼ FTE	¼ FTE	Survey	Cybersecurity Council office	Indiana General Assembly	Secretary of State should be involved.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Website space	Making documents available for review or download	May be within scope of current IN website maintenance	Unknown	Unknown	Unknown	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. By publishing details on types of services and insurance coverages available, Indiana will increase awareness and understanding of the need for cyber risk coverage.

b. By increasing the number of businesses protected against cybersecurity loss, Indiana's economy will be more resilient in the face of increasing cyber threats.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. It has been estimated that up to 60% of small and medium sized businesses fail within six (6) months of a cybersecurity attack. By encouraging small and medium sized businesses to protect against cybersecurity risks, Indiana companies will be better protected.

19. What is the risk or cost of not completing this deliverable?

a. Up to 60% of small and medium sized businesses fail within six (6) months of a cybersecurity attack and the risk of being targeted by an attack is rising exponentially. Indiana's economy could be damaged as the result of cyberattacks against Indiana businesses.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. There is no current survey of Indiana businesses on this subject. The Cybersecurity Council could work with (1) the Indiana Chamber of Commerce or (2) the Office of the Indiana Secretary of State to conduct a survey of Indiana businesses and use the increase of businesses covered by cybersecurity policies as a measure of success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No
b. **If Yes, please list states/jurisdictions**
    i. Other states or jurisdictions are likely looking at these statistics but we are not currently aware of concrete examples.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No
b. **If Yes, please list states/jurisdictions**
    i. We are not aware of initiatives in other states. But there may be.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None known

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No
b. **If Yes, what is the change and what could be the fiscal impact if the change is made**?
    i. N/A.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Surveys of Indiana businesses will require annual surveys or coordination with the Indiana Chamber of Commerce or the Office of the Indiana Secretary of State.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. No one outside of working group as of yet.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All sectors

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All stakeholders would benefit from this information.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. The Indiana Cybersecurity Office could coordinate with Office of the Indiana Attorney General's communications team.

Evaluation Methodology

Objective 1: Legal and Insurance Working Group conduct a survey of businesses for insurance coverage and cybersecurity insurance coverage by August 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Legal and Insurance Working Group provide a report of the findings of the cyber insurance survey to the IECC by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Cyber & Technology Insurance Guide - Version 1
- Survey of Cyber Laws

IECC Legal and Insurance Working Group

Cyber & Technology Insurance Guide Version 1

August 2018

CYBER & TECHNOLOGY INSURANCE COVERAGE

Today, consumers, businesses, and government agencies use internet-capable devices every day. These high tech devices – from laptops to security systems to medical devices – increase efficiency in the collection and exchange of data, and revolutionize industries. Cyber technology also brings new risks. Large companies subject to data breaches have made headlines, but small and mid-size companies that collect data and private information may also be vulnerable. Businesses may be obligated to protect private information by governing laws and regulations – such as Personally Identifiable Information, Personal Health Information and Confidential Corporate Information. Smaller businesses may not be able to survive the costs associated with a data breach. One of the largest growing financial risks a business must face is a cyber breach. Insurance is a necessary component of a business's risk management and disaster recovery plan. Inadequately insured businesses are unlikely to survive major incidents.

Until recently, most businesses have insured only computer equipment and mobile devices against physical risks such as damage, theft, or fire loss. Electronic equipment was insured on the same basis as furniture and automobiles, with no coverage for lost, stolen or disrupted data. Some organizations may have had wider, more extensive policies that also include coverage for equipment breakdown and limited expenses for reinstatement of data, but most cyber risks are now excluded under traditional commercial general liability policies.

Insurers and businesses have recognized that traditional insurance is inadequate, and there is a need for tailored cyber liability insurance to cover a wide variety of exposures that can result from technology-related activities -- from misplaced company cell phones to cyberattacks. Cyber liability insurance is intended to address an insured's obligation to protect private information from inappropriate access undergoing significant changes and likely will continue to do so as it is linked to the ever-changing world of technology. Therefore, it is important to know the terminology, to review your risks, and to determine your coverage needs. Cyber liability insurance is increasingly becoming an important consideration for conducting business in a high-tech marketplace.

FREQUENTLY ASKED QUESTIONS

Q What is cyber liability?

A Cyber liability is the risk of a data breach as a result of online activities and the use of electronic storage technology.

Q What is cyber liability insurance?

A While policies vary, cyber liability insurance is designed to protect a business or organization from:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private or confidential, such as employee, patient or customer records.

- Liability claims alleging invasion of privacy.
- Liability claims alleging failure of computer security that results in alterations of data and defense costs.

- Data Response Services, including legal, computer forensics, notification services, credit and identity monitoring products and crisis management expertise, and the reimbursement to the insured for certain out-of-pocket expenses.

Q What is a data breach?

A A data breach occurs when secured information is released to or accessed by unauthorized individuals. The lost data may be employee personnel records, customer financial accounts, or business trade secrets. The incidents pose serious risks for organizations as well as the individuals whose data has been lost or disseminated.

Q How do data breaches happen?

A Data breaches can occur by accident, such as an employee sends out an unsecured email, or by crime, such as a malicious hacker.

Q What data or information do businesses need to secure?

A Most businesses generate vast amounts of data which is available and stored on their electronic storage network systems, which may be subject to certain privacy laws:

- Personal information:
  - Personally identifiable information (PII): name, address, date of birth, telephone number, email address, Social Security number, zip code, biometric data.
  - Protected health information (PHI): healthcare-based treatment information, medical history, health insurance information, including member identification numbers.

- Corporate information: intellectual property, business, contracts, attorney-client privileged information:
  - Payment cardholder information (PCI): credit/debit card data, including account numbers, security codes, insurance account information, etc.

- Cyber-based data: web browser history, cookie information, metadata, and IP addresses.

Q Why consider cyber liability insurance?

A

There are various reasons why a company may want to consider cyber liability insurance as a way to protect confidential data and insure the risk against financial exposure:

- Frequency of privacy breaches are on the rise;
- Threats are getting dramatically worse;
- Almost all 50 states have enacted privacy laws in response to privacy breaches;
- Consumers expect that their confidential information will be protected.
- Class action litigation is becoming more active as a result of privacy breaches.
- Many business contracts now require cyber insurance.
- Cyber liability insurance products are becoming more widely available.

GLOSSARY OF CYBER INSURANCE TERMS

Breach Response – Investigation. Costs incurred to investigate data breach; investigate potential indemnity.

Breach Response – Notification. Costs incurred to notify individuals of breach.

Breach Response – Public Relations. Costs incurred to hire public relations firm.

Breach Response – Remediation. Costs incurred to remediate data breach (e.g., credit monitoring, call center, etc.).

Business Income (or Business Interruption Income Loss) is defined as net profit or loss before income taxes, as well as the continuing normal operating and payroll expenses.

Claim Expenses include reasonable and necessary legal fees, costs, and expenses incurred in the investigation, adjustment, defense, or appeal of a claim. They also typically include the cost of any bond or appeal bond required in any defended suit.

Computer System means computer hardware and software, and the electronic data stored thereon, as well as associated input and output devices, terminal devices, data storage devices, networking equipment, components, software, and electronic backup facilities, including systems accessible through the internet, intranets, extranets, or virtual private networks.

Cyber Attack (Denial of Service Attack) is action preventing an information system from functioning in accordance with its intended purpose; the inability of an authorized third party to access the company's Computer System; and the inability of an authorized third party to access his or her Computer System, where such inability is directly cause by the company's Computer System.

Cyber Extortion. Losses and expenses arising out of a criminal threat to release sensitive information or bring down a system/network.

Damages/Loss includes the amounts the business is legally obligated to pay as a result of a covered judgment, award, or settlement; costs charged against the business in any suit; or pre-

judgment and post-judgment interest and defense costs. It also includes punitive or exemplary damages where insurable by law.

Data Restoration – Security Failure. Costs to restore lost data caused by security failure.

Data Restoration – System Failure. Costs to restore lost data caused by system failure.

Denial of Service Attack is action preventing an information system from functioning in accordance with its intended purpose (see Cyber Attack).

Extra Expense means any reasonable and necessary expenses in excess of the business's normal operating expenses that the business incurs during the Period of Restoration associated with restoring and resuming operations, including securing temporary third-party Internet Service Provider services, temporary website and/or email hosting services, rental of temporary networks, or other temporary equipment or service contracts.

First Party Claim. A first party claim is brought by an insured under the insured's cyber policy for a loss that occurs because of loss or damage to the insured's business.

Funds Transfer and Computer Fraud – Social Engineering. Loss of money or property arising from *bona fide* wire instructions induced through social engineering.

Funds Transfer and Computer Fraud – Traditional Coverage. Loss of money or property arising from fraudulent wire instructions or fraudulent entries into a computer system.

Identity Restoration Services typically means consultation and assistance to an individual receiving notification services to determine whether identity theft has occurred, and, if so, to restore the individual's identity to pre-theft status.

Media or Electronic Publishing Incident means the actual or alleged unintentional libel, slander, trade libel, or disparagement resulting from the insured electronic publishing. It also includes plagiarism, violation of privacy, infringement of a copyright or trademark, or unauthorized use of titles formats, plots, or other protected material resulting from the insured's electronic or media publishing.

Media Liability. Claim by third party in connection with the insured's media content, which may include claim for trademark infringement, defamation, libel, product disparagement, copyright violation, or invasion of privacy.

Network/Computer System typically includes the computer hardware, software, and electronic data, as well as associated input and output devices, terminal devices, data storage devices, networking equipment, components, software, and electronic backup facilities, including systems accessible through the Internet, intranets, extranets, or virtual private networks.

Network Interruption – Contingent BI. Loss of income arising from business interruption caused by third-party service failure (including mitigation expenses).

Network Interruption – Security Failure. Loss of income arising from business interruption caused by security failure (including mitigation expenses).

Network Interruption – System Failure. Loss of income arising from business interruption caused by system failure (including mitigation expenses).

Network Security Liability. Claim by third party arising from the insured's failure of network security.

Network Security/Cyber Incident typically means any Unauthorized Access/Use of, or introduction of malicious code into, or Denial of Service Attack upon, the company's Computer System, that directly results in an interruption in services; or the corruption of deletion of digital assets.

Notification Services typically mean the preparation and distribution of notice letters from the insured advising individuals of the network security event and the availability of related resources if such notices are required by applicable law, as well as call center support services.

Period of Restoration is the period from which the business first suffered an interruption in service to the date and time it was restored (or could have been restored) with reasonable speed to substantially return to the level of operation that existed prior to the interruption. There is typically a limit on the policy that the period of restoration cannot exceed thirty days.

Personal Identifiable Information (PII) is information not available to the general public from which a person can be identified. This definition should be broad enough to include a person's name, telephone number, Social Security number, medical or healthcare data, driver's license number or state identification number, account number, credit and debit card number, or password.

Privacy Incident is the unintentional and unauthorized disclosure of Personal Identifiable Information or confidential information in the care, custody, or control of the business or service provider; a violation of a Privacy Regulation; or failure to comply with the term's own privacy policies.

Privacy Liability – Business Records Claim. Claim by third party arising from the insured's failure to protect trade secrets or other confidential business information.

Privacy Liability – Privacy Claim. Claim by third party arising from the insured's failure to protect personal information (including PII, PHI and FAI).

Privacy Liability – Regulatory Claims. Third party liability coverage that generally is designed to protect an insured business in connection with certain requests for information, investigative demands and/or civil proceedings often brought by or on behalf of a governmental agency arising from the insured's failure to protect personal information. The coverage often includes civil fines and penalties imposed on the insured, to the extent such fines and penalties are insurable by law.

Privacy Notification Costs are reasonable and necessary costs to hire a security expert to determine the existence and cause of a breach; costs to notify consumers under a breach notification law; or fees incurred to determine the actions necessary to comply with a breach notification law.

Privacy Regulation means statutes associate with the control and use of personally identifiable financial, medical, or other sensitive information.

Public Relations Expense typically means the hiring of a public relations firm or crisis management firm for communication services to explain the nature of the network security/cyber event and any corrective actions taken.

Regulatory Fines includes civil money penalties imposed by a federal, state, local, or foreign government entity pursuant to a regulatory proceeding.

Regulatory Proceeding is an investigation of an insured by an administrative, regulatory, or government agency concerning a Privacy Incident; or an administrative adjudicative proceeding for a privacy Wrongful Act or network security Wrongful Act.

Regulatory Injury means injury sustained by a person due to actual or alleged disparagement of an organization's products or services; libel or slander of natural person; or violation of such person's rights of privacy or publicity result from cyber activities.

Retroactive Date means the date in the declarations section of the policy. If no date is set forth in the declarations page, then the retroactive date is the date of the inception of the policy.

Reward Payment/Expenses/Cyber Extortion Costs means the reasonable amount paid by the business, with prior approval of the insurer, to an informant for information not otherwise available, which leads to the arrest and conviction of persons responsible for a cyber attack or threat covered under the policy.

Service Provider means a business the business does not own, operate or control, but that the insured hires and contracts to perform services related to the business' computer systems, including maintaining the computer system; hosting the business' internet website; handling, storing or destroying information and confidential materials; or providing other IT-related services.

Technology Errors & Omissions. Claim by third party for financial loss arising from errors or omissions in the technology-facing component of the insured's business (tech services or products).

Third Party Claim. A third party claim is a demand against the business for monetary damages or non-monetary relief; a written demand for arbitration; or a civil proceeding brought by the service of a complaint or similar pleading.

Unauthorized Access/Use is the use of, or access to, a computer system by a person unauthorized by the insured to do so, or the authorized use of, or access to, a Computer System in a manner not authorized by the insured.

Wrongful Act typically means the actual or alleged act, unintentional error, omission, neglect, or breach of duty by an insured business or Service Provider that directly results in a breach of the insured's network.

IECC Legal and Insurance Working Group

Survey of Cyber Laws

July 2018

Survey of Indiana Cyber Laws

Title or Description	Standard Type	Reference	Synopsis	Penalty	Statute of Limitations	Enforcement
IN Senate Bill 221 - E-Prescription Bill	State	SB 221	The bill requires prescribers to have access to and utilize INSPECT, a state-sponsored website database that allows practitioners to check a patient's controlled substance prescription history	https://iga.in.gov/legislative/2018/bills/senate/221		https://iga.in.gov/legislative/2018/bills/senate/221
IN Telephone Solicitation of Consumers ("Do Not Call Law")	State	IC art. 24-4.7	" A telephone solicitor may not make or cause to be made a telephone sales call to a telephone number if that telephone number appears in the most current quarterly listing published by the division." IC § 24-4.7-4-2.	$10,000 for the first call; $25,000 for subsequent calls. IC § 24-4.7-5-2(a)(2).	2 years after the call is made. IC § 24-4.7-5-4.	Attorney General: IC § 24-4.7-5-1.
IN Do Not Text Law	State	IC art. 24-4.7	"A telephone solicitor may not make or cause to be made a telephone sales call to a telephone number if that telephone number appears in the most current quarterly listing published by the division." IC § 24-4.7-4-2. A Telephone sales call can be defined as the "transmission of: a text message . . ." IC § 24-4.7-2-9(b)	$10,000 for the first call; $25,000 for subsequent calls. IC § 24-4.7-5-2(a)(2).	2 years after the call is made. IC § 24-4.7-5-4.	Attorney General: IC § 24-4.7-5-1.
IN Prohibited Spyware	State	IC art. 24-4.8	A person who is not the owner or operator of the computer may not knowingly or intentionally: (1) transmit computer software to the computer; and (2) by means of the computer software transmitted under subdivision (1), do any of the following" including deceptively modify computer settings or collect personally identifying information among other things. IC § 24-4.8-2-2.	Damages or $100,000: IC § 24-4.8-3-1(2).	Undefined by statute.	Private right of action: IC § 24-4.8-3-1.
IN Disclosure of Security Breach Act	State	IC art. 24-4.9	After a data security breach involving "personal information," a "data base owner" may need to alert (1) affected Indiana residents, (2) the attorney general, (3) consumer reporting agencies, and (4) the data base owner (if the breached party is not the data base owner). Must notify without unreasonable delay (likely within 30 days of the breach discovery). IC § 24-4.9.-3-1; IC § 24-4.9.-3-2.	$150,000 per notification type: IC § 24-4.9.-4-2(2)	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General: IC § 24-4.9-4-2
IN Protection of Personal Information	State	IC § 24-4.9-3-3.5(c)	"A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner." "A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act . . ."	$5,000 per deceptive act: IC § 24-4.9-3-3.5(c).	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General: IC § 24-4.9-3-3.5(f)
IN Disposal of Personal Information	State	IC § 24-4.9-3-3.5(d)	" A data base owner shall not dispose of or abandon records or documents containing unencrypted and unredacted personal information of Indiana residents without shredding, incinerating, mutilating, erasing, or otherwise rendering the personal information illegible or unusable."	$5,000 per deceptive act: IC § 24-4.9-3-3.5(c).	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General: IC § 24-4.9-3-3.5(f)
IN Disposal of Personal Information	State	IC § 24-4-14-8	"A person who disposes of the unencrypted, unredacted personal information of a customer without shredding, incinerating, mutilating, erasing, or otherwise rendering the information illegible or unusable commits a Class C infraction."	Class C or Class A infraction: IC § 24-4-14-8; 34-28-5-4	2 years: IC § 34-28-5-1(c)(2)	Prosecuting Attorney: IC § 34-28-5-1
IN Disposal of Electronic Waste	State	IC § 13-20.5-10-1	Covered entities cannot dispose of electronic in a landfill or through incineration	None: IC § 13-20.5-10-2	NA	NA
IN Deceptive Consumer Sales Act	State	IC ch. 24-5-0.5	"A supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act, omission, or practice by a supplier is a violation of this chapter whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations." IC § 24-5-0.5-3(a)	$5,000 per knowingly deceptive act: IC § 24-5-0.5-4(g)	2 years after the occurrence of the deceptive act: IC § 24-5-0.5-5.	Private Right of action and Attorney General: IC § 24-5-0.5-4(c)
IN Regulation of Automatic Dialing Machines	State	IC ch. 24-5-14	Indiana's Auto Dialer law prohibits most prerecorded calls, commonly known as "robo-calls," made via an automatic dialing-announcing device ("ADAD") regardless of the subject matter of the message. IC § 24-5-14-5(b).	$5,000 per knowingly deceptive act: IC § 24-5-0.5-4(g)	2 years after the occurrence of the deceptive act: IC § 24-5-0.5-5.	Attorney General: IC § 24-5-14-13.
IN Do Not Fax Law	State	IC § 24-5-0.5-3(b)(19).	Prohibition on sending unsolicited facsimile ("fax") advertisements . The law applies to advertisements sent to residential and business fax numbers. Unlike the Do Not Call law, the Do Not Fax law does not require people to register their fax numbers.	$5,000 per knowingly deceptive act: IC § 24-5-0.5-4(g)	2 years after the occurrence of the deceptive act: IC § 24-5-0.5-5.	Attorney General: IC § 24-5-14-13.

IN Deceptive Commercial Electronic Mail	State	IC ch. 24-5-22	Prohibition on sending unsolicited commercial electronic mail, when failing to comply with statutory sending standards. IC § 24-5-22-8.	Damages or $500 per email: IC § 24-5-22-10(d)(2).	Undefined by statute.	Private right of action: IC § 24-5-22-10(a).
IN Health Records and Identifying Information Protection	State	IC ch. 4-6-14	Provision relates to the Indiana Attorney General's responsibility related to abandoned health records and other records that contain personal information.	NA	NA	NA
IN Notice of Security Breach Act for State Agencies	State	IC ch. 4-1-11	"Any state agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person." IC § 4-1-11-5.	NA	NA	NA
IN Release of Social Security Numbers by State Agencies	State	IC § 4-1-10, et seq.	Details the scope of permissible disclosures of Social Security numbers as well as the consequences for violations of the statute.	Level 6 felony: IC § 4-1-10-8; Class A infraction: IC § 4-1-10-10.		Attorney General: IC §§ 4-1-10-11; 4-1-10-12.
IN Release of Social Security Numbers by State Agencies, Notice to Attorney General: Rules	Rule	10 IAC § 5-4-1	"When a state agency becomes aware of a release of Social Security numbers or other personal identifying information, the state agency or employee shall, within two (2) business days of the disclosure, notify the office of attorney general for the state in writing . . ."	NA	NA	NA
IN Driver's Privacy Protection Act ("DPPA")	State	IC § 9-14-13-2	Prohibits the disclosure of personal information associated with motor vehicle records by the Indiana Bureau of Motor Vehicles.	Class C misdemeanor: IC § 9-14-13-11	2 years: IC § 34-28-5-1(c)(2)	Prosecuting Attorney: IC § 33-39-1-5
IN Criminal Law - Wiretap Statute	State	IC art. 35-33.5	Provision outlines the requirements for the state to obtain a warrant to intercept the telephonic or telegraphic communications of an individual.	Suppression of Evidence: IC § 35-33.5-4-4.	NA	NA
IN Rights of Victims of Identity Deception: Civil	State	IC § 24-5-26-2	Provision outlines the duties of those that conduct trade or commerce concerning the protections for victims of identity theft.	$5,000: IC § 24-5-26-3	2 years from the mistreatment date: IC § 24-5-26-3	Attorney General: IC § 24-5-26-3
IN Rights of Victims of Identity Deception: Criminal	State	IC ch. 35-40-14	Provision outlines the duty of law enforcement agencies concerning identity theft and the protections for victims of identity theft.	NA	NA	NA
IN Criminal Law - Offense Against Intellectual Property	State	IC § 35-43-1-7	A person who knowingly or intentionally and who without authorization: (1) modifies data, a computer program, or supporting documentation; (2) destroys data, a computer program, or supporting documentation; or (3) discloses or takes data, a computer program, or supporting documentation that is: (A) a trade secret (as defined in IC 24-2-3-2); or (B) otherwise confidential as provided by law; and that resides or exists internally or externally on a computer, computer system, or computer network, commits an offense against intellectual property, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-5
IN Criminal Law - Offense Against Computer Users	State	IC § 35-43-1-8	(a) A person who knowingly or intentionally and who without authorization: (1) disrupts, denies, or causes the disruption or denial of computer system services to an authorized user of the computer system services that are: (A) owned by; (B) under contract to; or (C) operated for, on behalf of, or in conjunction with; another person in whole or part; (2) destroys, takes, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; (3) destroys or damages a computer, computer system, or computer network; or (4) introduces a computer contaminant into a computer, computer system, or computer network; commits an offense against computer users, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-6
IN Criminal Law - Identity Deception	State	IC § 35-43-5-3.5	(a) Except as provided in subsection (c), a person who knowingly or intentionally obtains, possesses, transfers, or uses the identifying information of another person, including the identifying information of a person who is deceased: (1) without the other person's consent; and (2) with intent to: (A) harm or defraud another person; (B) assume another person's identity; or (C) profess to be another person; commits identity deception, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-7

IN Criminal Law - Synthetic Identity Deception	State	IC § 35-43-5-3.8	(a) A person who knowingly or intentionally obtains, possesses, transfers, or uses the synthetic identifying information: (1) with intent to harm or defraud another person; (2) with intent to assume another person's identity; or (3) with intent to profess to be another person; commits synthetic identity deception, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-8
IN Criminal Law - Fraud	State	IC § 35-43-5-4	Encompasses different types of fraud including obtaining property by use of another's credit card unlawfully.	NA	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-9
IN Criminal Law - Unlawful Possession of a Card Skimming Device	State	IC § 35-43-5-4.3	A person who possesses a card skimming device with intent to commit: (1) identity deception (IC 35-43-5-3.5); (2) synthetic identity deception (IC 35-43-5-3.8); (3) fraud (IC 35-43-5-4); or (4) terroristic deception (IC 35-43-5-3.6); commits unlawful possession of a card skimming device. Unlawful possession of a card skimming device under subdivision (1), (2), or (3) is a Level 6 felony. Unlawful possession of a card skimming device under subdivision (4) is a Level 5 felony.	Level 5 Felony: IC § 35-50-2-6	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-10
IN Unlawful Recording	State	IC § 35-46-8-4	"A person who knowingly or intentionally uses an audiovisual recording device in a motion picture exhibition facility with the intent to transmit or record a motion picture commits unlawful recording, a Class B misdemeanor."	Class B misdemeanor: IC § 35-50-3-3	2 years: IC § 35-41-4-2(a)(2)	Prosecuting Attorney: IC § 33-39-1-11
IN Unlawful Photography and Surveillance of Private Property	State	IC § 35-46-8.5-1	"A person who knowingly or intentionally places a camera or electronic surveillance equipment that records images or data of any kind while unattended on the private property of another person without the consent of the owner or tenant of the private property commits a Class A misdemeanor." Note: Numerous exceptions enumerated within the statute.	Class A misdemeanor: IC § 35-50-3-2	2 years: IC § 35-41-4-2(a)(2)	Prosecuting Attorney: IC § 33-39-1-12
IN State Insurance Commissioners **Navigators and Application Organizations**	State	760 IAC § 4-5-2	"Navigators and application organizations shall comply with the following safeguards to maintain and protect the confidentiality of personal information:"	Up to $10,000 per violation: 760 IAC § 4-7-1(d)	NA	If a navigator or application organization does not comply with the requirements of this rule, the commissioner may initiate an enforcement action against the navigator or application organization under 760 IAC 4-7.
IN Department of Financial Institutions ("DFI")	State		Enforces FFIEC standards.			

Survey of Federal Cyber Laws

Date	Title	Subtitle	Reference	Information
1914	Executive Order 13571		15 U.S.C. § 45, et seq.	Gave the FTC the authority to enforce rules prohibiting “unfair or deceptive acts or practices in or affecting commerce."
		FTC Section 5 Authority	15 U.S.C. § 45(a)(1), et seq.	The basic consumer protection statute enforced by the Commission is Section 5(a) of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce...are...declared unlawful."
1966	Freedom of Information Act (FOIA) of 1966		5 U.S.C. § 552, et seq.	Under FOIA, “any person” may request “records” maintained by an executive agency. People or entities requesting records need not state a reason for requesting records. Today, all fifty states have freedom of information laws, many of which are based upon the FOIA.
1968	Wiretap Act of 1968		8 U.S.C. § 2511, et seq.	Broadly prohibits the intentional interception, use, or disclosure of wire and electronic communications unless a statutory exception applies. In general, these prohibitions bar unauthorized third parties (including the government) from wiretapping telephones and installing electronic "sniffers" that read Internet traffic.
1968	Omnibus Crime and Control and Safe Streets Act of 1968		18 U.S.C. §§ 2510–22, et seq.	Extended the reach of wiretap regulations to state officials as well as to private parties. Despite its profound increase in the extent of protection, Title III had important limitations. It applied to the interception of “aural” communications; it did not apply to visual surveillance or other forms of electronic communication.
1970	Fair Credit Reporting Act of 1970		15 U.S.C. § 1681, et seq.	The Fair Credit Reporting Act (FCRA) provides limited protections for individuals. It enables people to access their records, and restricts the manner in which records are disclosed. Individuals can challenge inaccuracies on their reports and can sue to collect damages for violations of the Act. However, FCRA immunizes creditors and credit reporting agencies from lawsuits for “defamation, invasion of privacy, or negligence” except when the information is “furnished with malice or willful intent to injure such consumer.” Although the FCRA allows people to sue for negligent violations of the Act, there is a two-year statute of limitations “from the date on which the liability arises."
1970	Racketeer Influenced and Corrupt Organization (RICO) Act of 1970		118 U.S.C. ch. 96	Passed in 1970, the Racketeer Influenced and Corrupt Organizations Act (RICO) is a federal law designed to combat organized crime in the United States. It allows prosecution and civil penalties for racketeering activity performed as part of an ongoing criminal enterprise. Such activity may include illegal gambling, bribery, kidnapping, murder, money laundering, counterfeiting, embezzlement, drug trafficking, slavery, and a host of other unsavory business practices.

1970	Bank Secrecy Act of 1970		Pub. L. No. 91-508 12 U.S.C. §§ 1730(d), 1829b, 1951-59, et seq. 31 U.S.C. H9 1051-1122, et seq.	The Bank Secrecy Act, enacted in 1970, requires banks to retain records and create reports to help law enforcement investigations. The Act was passed due to concerns that the computerization of records would make white collar crime more difficult to detect. Federally insured banks must record the identities of account holders and maintain copies of each financial instrument. International transactions exceeding $5,000 are subject to reporting, as well as domestic transactions exceeding $10,000. In *California Bankers Ass'n v. Shultz* , 416 U.S. 21 (1974), the Supreme Court upheld the Act against a Fourth Amendment challenge by a group of bankers and account holders. The Court concluded that the bankers lacked Fourth Amendment rights in the data because "corporations can claim no equality with individuals in the enjoyment of a right to privacy." *Id* at 65. The account holders failed to allege that they engaged in transactions exceeding $10,000, and as a result, lacked standing.
1974	Privacy Act of 1974		5 U.S.C. § 552a, et seq.	The Act responded to many of the concerns raised by the United States Department of Health Education and Welfare (HEW) report, "Records, Computers, and the Rights of Citizens." It regulates the collection and use of records by federal agencies, and affords individuals right to access and correct their personal information.
1974	Family Educational Rights and Privacy Act of 1974		20 U.S.C. § 1232g, et seq.	The Family Educational Rights and Privacy Act of 1974 (FERPA), otherwise known as the "Buckley Amendment," regulates the accessibility of student records. FERPA does not apply to records maintained by school law enforcement officials or health and psychological records.
1978	Protection of Pupil Rights Amendment ("PPRA") of 1978		20 U.S.C. § 1232h, et seq.; 34 C.F.R. part 98, et seq.	PPRA is a federal law that affords certain rights to parents of minor students with regard to surveys that ask questions of a personal nature. Briefly, the law requires that schools obtain written consent from parents before minor students are required to participate in any U.S. Department of Education funded survey, analysis, or evaluation that reveals information certain topics.
1978	Foreign Intelligence Surveillance Act of 1978		50 U.S.C. §§ 1801–11, et seq.	The Foreign Intelligence Surveillance Act (FISA) of 1978, created a distinct regime for electronic surveillance to gather foreign intelligence. Whereas Title III regulated electronic surveillance for domestic law enforcement purposes, FISA applied when foreign intelligence gathering was "the purpose" of the investigation. FISA permits electronic surveillance and covert searches pursuant to court orders, which are reviewed ex parte by a special court of seven federal judges.
1978	Right to Financial Privacy Act of 1978		29 U.S.C. § 3407, et seq.	The Right to Financial Privacy Act (RFPA) provided limited protection of financial records to fill the gap left by *United States v. Miller* , 425 U.S. 435, 435 (1976). Pursuant to the RFPA, government officials must use a warrant or subpoena to obtain financial information. There must be "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry." Subject to certain exceptions, the customer must receive prior notice of the subpoena.
1978	Airline Deregulation Act - Preemption of authority over prices, routes, and service		49 U.S.C.A. § 41713, et seq.	"[A] State, political subdivision of a State, or political authority of at least 2 States may not enact or enforce a law, regulation, or other provision having the force and effect of law related to a price, route, or service of an air carrier that may provide air transportation under this subpart."

1979	Drug Abuse Prevention, Treatment, and Rehabilitation Act of 1979		42 C.F.R. part 2, et seq.	Drug Abuse Prevention, Treatment, and Rehabilitation Act (Act) is a federal statute designed to be a practical resource for governments, policy planners, service commissioners and treatment providers against drug abuse. The Act makes provision for federal drug abuse programs and activities. The Act also provides for education, treatment, rehabilitation, research, training, and law enforcement efforts to prevent drug abuse.
1980	Privacy Protection Act of 1980		42 U.S.C. § 2000aa, et seq.	Dissatisfaction over *Zurcher v. Stanford Daily* , 436 U.S. 547 (1978) led Congress to pass the Privacy Protection Act in 1980. The Act restricts the search or seizure of "any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." As a result of the Act, a subpoena is needed to obtain work product materials, which permits the party to challenge the request in court and to produce the documents without having law enforcement officials intrude on the premises.
1984	Cable Communications Policy Act of 1984		42 U.S.C. § 551, et seq.	The Cable Communications Policy Act (CCPA) of 1984 protects the privacy of cable records. Cable companies must notify subscribers about the collection and use of personal information. Companies cannot disclose a subscriber 's viewing habits. The Act is enforced with a private right of action.
1986	Computer Fraud and Abuse Act of 1986		18 U.S.C. § 1030, et seq.	A United States cybersecurity bill that was enacted in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984. The law prohibits accessing a computer without authorization, or in excess of authorization. The original 1984 bill was enacted in response to concern that computer-related crimes might go unpunished. The House Committee Report to the original computer crime bill characterized the 1983 techno-thriller film WarGames—in which a young Matthew Broderick breaks into a U.S. military supercomputer programmed to predict possible outcomes of nuclear war and unwittingly almost starts World War III—as "a realistic representation of the automatic dialing and access capabilities of the personal computer."
1988	Computer Matching and Privacy Protection Act of 1988		5 U.S.C. § 552a(a)(8)–(13), (e)(12), (o)–(r), (u)), et seq.	A major loophole in the Privacy Act of 1974 has been the "routine use" exception. Under this exception, to detect fraud, the federal government in 1977 began running computer comparisons of employee records with the records of people receiving benefits. In 1988, Congress addressed this practice, known as "computer matching" by passing the Computer Matching and Privacy Protection Act. The law established procedures for computer matchings, but did not halt the practice.
1988	Employee Polygraph Protection Act of 1988		29 U.S.C. §§ 2001-09, et seq.	In 1988, Congress passed the Employee Polygraph Protection Act (EPPA). The EPPA prohibits private sector employers from using polygraph examinations on employees and prospective employees. The Act does not apply to public sector employers. Employers can, however, use polygraphs "in connection with an ongoing investigation involving economic loss or injury to the employer's business, such as theft, embezzlement, misappropriation, or an act of unlawful industrial espionage or sabotage" when "the employer has a reasonable suspicion that the employee was involved in the incident or activity under investigation." Private sector employers who provide security services are exempt.

1988	Video Privacy Protection Act of 1988		18 U.S.C. § 2710(b), et seq.	The confirmation hearings of Supreme Court Justice nominee Robert Bork sparked a law to protect videocassette rental data. Reporters attempted to obtain a list of the videos Bork had rented from his video store. Incensed at this practice, Congress passed the Video Privacy Protection Act (VPPA) of 1988.251 The VPPA forbids videotape service providers from disclosing customer video rental or purchase information.
1986	Electronic Communications Privacy Act of 1986		18 U.S.C. §§ 2510-22, 2701-11, 3121-27, et seq.	In 1986, Congress revisited its wiretapping law by substantially reworking Title III of 1968. The Electronic Communications Privacy Act (ECPA) expanded Title III to new forms of communications, with a particular focus on computers. The ECPA restricts the interception of transmitted communications and the searching of stored communications. Title I of the ECPA, known as the "Wiretap Act," regulates the interception of communications. Title II, referred to as the "Stored Communications Act," governs access to stored communications and records held by communications service providers (such as ISPs). Title III, called the "Pen Register Act," provides limited regulation of pen registers and trap and trace devices.
1991	Telephone Consumer Protection Act of 1991		47 U.S.C. § 227, et seq.	In 1991, Congress enacted the Telephone Consumer Protection Act (TCPA), which permits people to request that telemarketers not call them again. If the telemarketer continues to call, people can sue for damages of up to $500 for each call.
1993	Government Performance and Results Act of 1993		Pub. L. No. 103-62	Requires executive agency heads to submit to the Director of the Office of Management and Budget (OMB) and the Congress a strategic plan for performance goals of their agency's program activities. Requires such plan to cover at least a five-year period and to be updated at least every three years. See: https://www.congress.gov/bill/103rd-congress/senate-bill/20
1994	Driver's Privacy Protection Act of 1994		18 U.S.C. §§ 2721-25, et seq.	In 1994, Congress passed the Driver 's Privacy Protection Act (DPPA), which requires that states first obtain a person's consent before disclosing her motor vehicle record information to marketers.
1995	Paperwork Reduction Act (PRA) of 2005		44 U.S.C. § 3501, et seq.	Designed to reduce the public's burden of answering unnecessary, duplicative, and burdensome government surveys.
1996	Health Insurance Portability and Accountability Act (HIPAA) of 1996		Pub. L. No. 104-191, 110 Stat. 1936	The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the first federal statute to directly address health privacy. HIPPA required the Department of Health and Human Services (HHS) to draft regulations to protect the privacy of medical records. HHS's regulations, among other things, require that people authorize all uses and disclosures of their health information that are not for treatment, payment, or health care operation (such as for marketing purposes).

		HIPAA Privacy Rule	45 C.F.R. part 160, et seq. and 45 C.F.R. part 164, subparts A and E, et seq.	The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
		HIPAA Security Rule	45 C.F.R. part 160 and 45 C.F.R. part 164, subparts A and C, et seq.	The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
		HIPAA Breach Notification Rule	45 CFR part 164, subpart D, et seq.	Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
		Uses and disclosures for which an authorization or opportunity to agree or object is not required.	45 C.F.R. § 164.512, et seq.	Provides when covered entities or business associates are nor required to obtain valid authorization to use or disclose protected health information. General exceptions exist for public health activities.
		Uses and disclosures to carry out treatment, payment, or health care operations.	45 C.F.R. § 164.506, et seq.	Provides when covered entities or business associates are nor required to obtain valid authorization to use or disclose protected health information. General exceptions exist for collection of payments for medical services.
		Imposition of Civil Money Penalties	45 CFR, part 160, subpart D, et seq.	Provides guidelines for determining what amount an entity should be penalized for violating HIPAA.
1996	Economic Espionage Act of 1996		8 U.S.C. §§ 1831-39, et seq.	This regulation is intended to protect from disclosure outside the government proprietary information that is provided to the government during a bidding process. Exemption 4 of the Freedom of Information Act exempts from mandatory disclosure information such as trade secrets and commercial or financial information obtained by the government from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness. The law on Disclosure of Confidential Information (18 U.S.C. § 1905) makes it a crime for a federal employee to disclose such information.

1997	No Electronic Theft Act of 1997		Pub. L. No. 105-147	Provides for criminal prosecution of individuals who engage in copyright infringement under certain circumstances, even when there is no monetary profit or commercial benefit from the infringement.
1998	Children's Online Privacy Protection Act of 1998		15 U.S.C. §§ 6501-06, et seq.	The Children's Online Privacy Protection Act (COPPA) of 1998 governs the collection of children's personal information on the Internet. The law only applies to children under the age of thirteen. Children's websites must post privacy policies and obtain "parental consent for the collection, use, or disclosure of personal information from "children." COPPA applies only to websites "directed to children" or where the operator of the website "has actual knowledge that it is collecting personal information from a child."
1998	Digital Millennium Copyright Act (DMCA) of 1998		Pub. L. No. 105-304; 17 U.S.C. §§ 101, 104, 104A, 108, 112, 114, 117, 701, et seq.; 17 U.S.C. §§ 512, 1201–1205, 1301–1332, et seq.; 28 U.S.C. § 4001, et seq.	A U.S. copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works (commonly known as digital rights management or DRM). It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet.
1999	U.S. Uniform Computer Information Transactions Act (UCITA) of 1999 (Last Amended or Revised in 2002)		Uniform Laws Annotated. Uniform Computer Information Transactions Act (Last Amended or Revised in 2002)	UCITA provides a comprehensive set of rules for licensing computer information, whether computer software or other clearly identified forms of computer information. Computerized databases and computerized music are other examples of computer information that would be subject to UCITA. It would also govern access contracts to sites containing computer information, whether on or off the Internet. UCITA would also apply to storage devices, such as disks and CDs that exist only to hold computer information. Professional services by a member of a regulated profession (doctor, lawyer, accountant, for example) are not within UCITA even though communications about the transaction will be in the form of computer information.
1999	The Gramm-Leach-Bliley Act of 1999		15 U.S.C. § 6802(a)-(b), et seq.	In 1999, Congress passed the Gramm-Leach-Bliley (GLB) Act, which allows financial institutions with different branches or affiliates engaging in different services to share the "nonpublic personal information" among each branch of the company. Affiliates must inform customers of the information sharing, but people have no right to stop the companies from sharing it. However, when financial institutions desire to share customer data with third parties, people have a right to opt-out.

2000	Security and Exchange Commission ("SEC") Privacy of Consumer Financial Information Regulations of 2000		17 C.F.R. part 248, subpart A, et seq.	The SEC adopted Regulation S-P, privacy rules promulgated under section 504 of the Gramm-Leach-Bliley Act. Section 504 of GLBA required the Commission to adopt rules implementing notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers. The Regulation implements these requirements of the GLBA with respect to investment advisers registered with the Commission, brokers, dealers, and investment companies, which are the financial institutions subject to the Commission's jurisdiction under that Act.
2000	U.S. Congress Electronic Signatures in Global National ("ESIGN") Commerce Act of 2000		Pub. L. No. 106–229	The ESIGN Act is a landmark federal law in the United States. Passed in 2000, it granted legal recognition to electronic signatures and records in the USA based on the understanding that if all parties to a contract choose to use electronic documents and to sign them electronically, they are legal. The ESIGN Act (along with its precursor UETA) provided the legal foundation for use of electronic records and electronic signatures in commerce. It confirmed that electronic records and signatures carry the same weight and have the same legal effect as traditional paper documents and wet ink signatures.
2001	The U.S. Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001		Pub. L. No. 107-56	In a very short time after the September 11 terrorist attack, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (USA PATRIOT Act) of 2001. The Act made several significant changes to the ECPA and FISA, among other statutes. In one amendment, the USA PATRIOT Act enlarged the definition of pen registers and trap and trace devices to apply to addressing information on emails and to "IP addresses." The Act also provided for new justifications for delayed notice of search warrants, increasing the types of subscriber records that could be obtained from ISPs and communications providers, and allowing for a nationwide scope for pen register orders and search warrants for email. The Act also provided for roving wiretaps under FISA as well as increased sharing of foreign intelligence information between law enforcement entities.
2002	Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002		44 U.S.C. § 101	CIPSEA establishes uniform confidentiality protections for information collected for statistical purposes by U.S. statistical agencies, and it allows some data sharing between the Bureau of Labor Statistics, Bureau of Economic Analysis, and Census Bureau. The agencies report to OMB on particular actions related to confidentiality and data sharing. The law give the agencies standardized approaches to protecting information from respondents so that it will not be exposed in ways that lead to inappropriate or surprising identification of the respondent. By default the respondent's data is used for statistical purposes only. If the respondent gives informed consent, the data can be put to some other use.
2002	Sarbanes-Oxley Act ("SOX") of 2002		15 U.S.C. ch. 2A, 98, et seq.	SOX protects shareholders and the general public from accounting errors and fraudulent practices of organizations. It was also tailored to improve the accuracy of corporate disclosures. SOX compliance has recently shifted to include cybersecurity.

2002	E-Government Act of 2002		44 U.S.C. § 3601, et seq.	Established procedures to ensure the privacy of personal information in electronic records. Section 208 of the E-Government Act of 2002 requires agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. PIAs must be made publicly available, unless the agency determines not to make the PIA publicly available if such publication would raise security concerns, reveal classified (i.e., national security), or reveal sensitive information (e.g., potentially damaging to a national interest, law enforcement effort, or competitive business interest).
2002	The Homeland Security Act of 2002		6 U.S.C. § 222, et seq.	In 2002, Congress passed the Homeland Security Act, which created the Department of Homeland Security (DHS), consisting of twenty-two federal agencies. The Act created a Privacy Office for ensuring compliance with privacy laws.
2002	Federal Information Security Management Act ("FISMA") of 2002		44 U.S.C. § 3551, et seq.	FISMA is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA assigns responsibilities to various agencies to ensure the security of data in the federal government. The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely and efficient manner.
2003	Do-Not-Call Implementation Act (National Do-Not-Call Registery) of 2003		15 U.S.C. ch. 87-87A, et seq.	In an effort to address unwanted telemarketing calls, the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) created a do-not-call registry. People can voluntarily register their telephone numbers, and commercial telemarketers are prohibited from calling the numbers. Telemarketers challenged the do-not-call registry as a violation of their First Amendment rights. In 2004, a federal circuit court concluded in *Mainstream Marketing Services, Inc. v. Federal Trade Commission* , 358 F.3d 1228 (10th Cir. 2004) that the do-not-call registry satisfied the *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York* , 447 U.S. 557 (1980) balancing test for commercial speech and therefore did not run afoul of the First Amendment.
2003	The CAN-SPAM Act of 2003		15 U.S.C. § 7701, et seq.	The Act establishes requirements for those who send unsolicited commercial email. The Act bans false or misleading header information and prohibits deceptive subject lines. It also requires that unsolicited commercial email be identified as advertising and provide recipients with a method for opting out of receiving any such email in the future. In addition, the Act directs the FTC to issue rules requiring the labeling of sexually explicit commercial email as such and establishing the criteria for determining the primary purpose of a commercial email.
2003	The Fair and Accurate Credit Transactions Act of 2003		Pub. L. No. 108-159	In 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which amended the Fair Credit Reporting Act and extended its preemption on certain state law provisions addressing identity theft and credit reporting. Among other things, the FACTA provided some limited protections against identity theft. For example, FACTA requires credit reporting agencies to provide people with a free credit report each year. It requires credit reporting agencies to disclose to a consumer her credit score, and it allows victims of fraud to alert just one credit reporting agency, which then must notify the others. These provisions and others were criticized by many as not going far enough to address the problem of identity theft.

2004	The Intelligence Reform and Terrorism Prevention Act of 2004		Pub. L. No. 108-458	In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act to facilitate greater information sharing between federal agencies. The Act requires that intelligence be "provided in its most shareable form" and it aims to "promote a culture of information sharing.
2005	The Real ID Act of 2005		Pub. L. No. 109-13	Attached to a military spending bill, and passed without debate, the Real ID Act of 2005 mandated that state driver 's licenses meet federal standards set forth by the DHS. Critics claimed that it would establish a de facto national identification card and that it would be extremely costly for the states to implement.
2006	U.S. SAFE WEB Act of 2006		15 U.S.C. §§ 45-58, et seq.	This Act, amending the FTC Act of 1914, provides the FTC with a number of tools to improve enforcement regarding consumer protection matters, particularly those with an international dimension, including increased cooperation with foreign law enforcement authorities through confidential information sharing and provision of investigative assistance. The Act also allows enhanced staff exchanges and other international cooperative efforts.
2007	Open Government Act of 2007		Public Law No. 110-175; 5 U.S.C. § 552, et seq.	Promotes accessibility, accountability, and openness in Government by strengthening 5 U.S.C. § 552 and codifies several provisions of Executive Order 13,392, "Improving Agency Disclosure of Information."
2007	The Freedom of Information Act (FOIA) of 2007		5 U.S.C. § 552, et seq.	Amended Freedom of Information Act (FOIA) of 1966. Provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions.
2008	Genetic Information Nondiscrimination Act ("GINA") of 2008		15 U.S.C. §§ 2000ff - 2000ff(11), et seq.	GINA protects individuals against discrimination based on their genetic information in health coverage and in employment. GINA is divided into two sections, or Titles. Title I of GINA prohibits discrimination based on genetic information in health coverage. Title II of GINA prohibits discrimination based on genetic information in employment.
2009	Health Information Technology for Economic and Clinical Health Act ("HITECH Act")		42 C.F.R. parts 412, 413, 422, and 495, et seq.	Promotes the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.
		Access to systems and records.	42 C.F.R. § 495.346, et seq.	"The State agency must allow HHS access to all records and systems operated by the State in support of this program, including cost records associated with approved administrative funding and incentive payments to Medicaid providers. State records related to contractors employed for the purpose of assisting with implementation or oversight activities or providing assistance, at such intervals as are deemed necessary by the Department to determine whether the conditions for approval are being met and to determine the efficiency, economy, and effectiveness of the program."

		Combating fraud and abuse.	42 C.F.R. § 495.368, et seq.	"(a) General rule. (1) The State must comply with Federal requirements to— (i) Ensure the qualifications of the providers who request Medicaid EHR incentive payments; (ii) Detect improper payments; and (iii) In accordance with § 455.15 and § 455.21 of this chapter, refer suspected cases of fraud and abuse to the Medicaid Fraud Control Unit. (2) The State must take corrective action in the case of improper EHR payment incentives to Medicaid providers."
2010	Government Performance and Results Modernization (GPRM) Act of 2010 (Amends the Government Performance and Results Act of 1993)		Pub. L. No. 111-352 (Amends the Government Performance and Results Act of 1993)	Amends the Government Performance and Results Act of 1993 to require each executive agency to make its strategic plan available on its public website on the first Monday in February of any year following that in which the term of the President commences and to notify the President and Congress. Requires such plan to cover at least a four-year period and to include a description of how the agency is working with other agencies to achieve its goals and objectives, as well as relevant federal government priority goals. Requires the Director of the Office of Management and Budget (OMB) to coordinate with agencies to develop a federal government performance plan, which shall be submitted with the annual federal budget and concurrently made available on an OMB website of agency programs. Requires such plan to: (1) establish government performance goals for the current and next fiscal years; (2) identify activities, entities, and policies contributing to each goal; (3) identify a lead government official responsible for coordinating efforts to achieve the goal; (4) establish common federal government performance indicators with quarterly targets; (5) establish clearly defined quarterly milestones; and (6) identify major management
2014	Federal Information Security Modernization Act of 2014		44 U.S.C. § 3541, et seq.	This Act amends the Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, and requires agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of an agency.
2017	Social Security Number Fraud Prevention Act of 2017		Pub. L. No. 115-59	This Act: (1) prohibits federal agencies from including any individual's Social Security account number on any document sent by mail unless the agency head determines that such inclusion is necessary; and (2) requires agencies that have Chief Financial Officers to issue regulations, within five years of this bill's enactment, that specify the circumstances under which such inclusion is necessary.
2017	The Protecting Patient Access to Emergency Medications Act of 2017		21 U.S.C. § 823, et seq.	In 1970, the Controlled Substances Act (CSA) was created to regulate substances that have the potential to be abused. At the time, the CSA lacked instructions for the maintenance and use of these substances by emergency medical services (EMS). States, therefore, created their own EMS-related controlled substances requirements. In 2017, the Protecting Patient Access to Emergency Medications Act (PPAEMA) was introduced in the United States Congress to amend the CSA to include EMS requirements and end confusion among states and EMS agencies. The PPAEMA was signed into law on November 17, 2017.

2018	Defense Federal Acquisition Regulation Supplement ("DFARS")		48 C.F.R. § 201.104, et seq.	DFARS Safeguarding riles and clauses, for the basic safeguarding of contractor information systems that process, store or transmit Federal contract information. DFARS provides a set of "basic" security controls for contractor information systems upon which this information resides. These security controls must be implemented at both the contractor and subcontractor levels based on the information security guidance in NIST Special Publication 800-171 "Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations."

FEDERAL AGENCY POLICIES

Date	Title	Subtitle	Reference	Information
1973	Organization of Economic Cooperation and Development (OECD) Fair Information Practices		U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems 29 (1973)	The OCED Fair Information Practices were articulated by the United States Department of Health Education and Welfare (HEW) in 1973. HEW investigated the issues with increasing computerization of information and growing depositories of personal data. The report recommended the page of a code of Fair Information Practices, which were later codified in the Privacy Act of 1974. The recommended practices included the following: 1. There must be no personal data record-keeping systems whose very existence is secret. 2. There must be a way for an individual to find out what information about him is in a record and how it is used. 3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent. 4. There must be a way for an individual to correct or amend a record of identifiable information about him. 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

1980	Organization of Economic Cooperation and Development (OECD) Privacy Guidelines		Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available in Marc Rotenburg, Privacy Law Sourcebook (2002)	The OECD Privacy Guidelines built upon the Fair Information Practices articulated by the United States Department of Health Education and Welfare (HEW). The OECD Guidelines contain eight principles: (1) collection limitation—data should be collected lawfully with the individual's consent; (2) data quality—data should be relevant to a particular purpose and be accurate; (3) purpose specification—the purpose for data collection should be stated at the time of the data collection and the use of the data should be limited to this purpose; (4) use limitation—data should not be disclosed for different purposes without the consent of the individual; (5) security safeguards—data should be protected by reasonable safeguards; (6) openness principle—individuals should be informed about the practices and polices of those handling their personal information; (7) individual participation—people should be able to learn about the data that an entity possesses about them and to rectify errors or problems in that data; (8) accountability—the entities that control personal information should be held accountable for carrying out these principles.

Survey of Other States Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement
Alabama Breach Notification Law	Ala. Code § 8-38-5	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 people • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 10,000 residents or $500,000 • Credit Monitoring: No	$500,000 and $5,000 per day: Ala. Code § 8-38-9	Attorney General: Ala. Code § 8-38-9
Alabama Personal Information Protection Act	Ala. Code § 8-38-3	"Each covered entity and third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security."	Most likely, this would be considered a deceptive practice under Ala. Code § 8-19-5.	None
Alabama Unfair, Deceptive, or Abusive Acts and Practices	Ala. Code § 8-19-5	"The following deceptive acts or practices in the conduct of any trade or commerce are hereby declared to be unlawful: . . . (27) Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce."	Up to $2,000 per violation: Ala. Code § 8-19-11	Attorney General: Ala. Code § 8-19-4
Alaska Breach Notification Law	Alaska Stat. § 45.48.010	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if not disclosing to residents • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Unclear • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 300,000 residents or $150,000 • Credit Monitoring: No	Up to $50,000: Alaska Stat. § 45.48.080(b)(1)	Attorney General: Alaska Stat. § 44.23.020(b)(4)
Alaska Personal Information Protection Act	Alaska Stat. § 45.48.430	"A person doing business, including the business of government, may not disclose an individual's social security number to a third party."	Up to $3,000: Alaska Stat. § 45.48.480	Attorney General: Alaska Stat. § 44.23.020(b)(4)
Alaska Unfair, Deceptive, or Abusive Acts and Practices	Alaska Stat. § 45.50.471	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce are declared to be unlawful."	Between $1,000 and $25,000 per violation: Alaska Stat. § 45.50.537	Attorney General: Alaska Stat. § 45.50.501
Arizona Breach Notification Law	Ariz. Rev. Stat. § 18-545	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 100,000 people or $50,000 • Credit Monitoring: No	$10,000 per breach: Ariz. Rev. Stat. § 18-545(H)	Attorney General: Ariz. Rev. Stat. § 18-545(H)
Arizona Unfair, Deceptive, or Abusive Acts and Practices	Rev. Stat. § 44-1522	"The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice."	Up to $10,000 per violation: Ariz. Rev. Stat. § 44-1531	Attorney General: Ariz. Rev. Stat. § 44-1524
Arkansas Breach Notification Law	Ark. Code § 4-110-105	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: No •	Up to $10,000 per violation: Ark. Code §§ 4-110-108; 4-88-113	Attorney General: Ark. Code Ark. Code §§ 4-110-108;§ 4-88-104

Arkansas Personal Information Protection Act	Ark. Code § 4-110-104(b)	"A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure"	Up to $10,000 per violation: Ark. Code §§ 4-110-108; 4-88-113	Attorney General: Ark. Code Ark. Code §§ 4-110-108;§ 4-88-104
Arkansas Unfair, Deceptive, or Abusive Acts and Practices	Ark. Code § 4-88-108	"When utilized in connection with the sale or advertisement of any goods, services, or charitable solicitation, the following shall be unlawful: (1) The act, use, or employment by any person of any deception, fraud, or false pretense; or (2) The concealment, suppression, or omission of any material fact with intent that others rely upon the concealment, suppression, or omission."	Up to $10,000 per violation: Ark. Code § 4-88-113	Attorney General: Ark. Code § 4-88-104
California Breach Notification Law	Cal. Civ. Code § 1798.82	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: • Credit Monitoring: • Other:	Up to $3,000 per transaction: Cal. Civ. Code § 1798.84	Private right of action: Cal. Civ. Code § 1798.84
California Personal Information Protection Act	Cal. Civ. Code § 1798.81.5	"A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."	Up to $3,000 per transaction: Cal. Civ. Code § 1798.84	Private right of action: Cal. Civ. Code § 1798.84
California Unfair, Deceptive, or Abusive Acts and Practices	Cal. Bus. & Prof. Code § 17200	"As used in this chapter, unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code."	$2,500 per violation: Cal. Bus. & Prof. Code § 17206	Attorney General: Cal. Bus. & Prof. Code § 17206
Colorado Breach Notification Law	Colo. Rev. Stat. § 6-1-716	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 250,000 residents or $250,000 • Credit Monitoring: No	"The attorney general may bring an action in law or equity to address violations of this section and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law." Colo. Rev. Stat. § 6-1-716(4)	Attorney General: Colo. Rev. Stat. § 6-1-716(4)
Colorado Unfair, Deceptive, or Abusive Acts and Practices	Colo. Rev. Stat. § 6-1-105	"A person engages in a deceptive trade practice when, in the course of the person's business, vocation, or occupation, the person:"	Up to $2,000 per violation: Colo. Rev. Stat. § 6-1-112	Attorney General: Colo. Rev. Stat. § 6-1-103.
Connecticut Breach Notification Law	Conn. Gen. Stat. § 36a-701b	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: Yes, 12 months • Other:	Up to $5,000 per violation: Conn. Gen. Stat. §§ 36a-701b(g), 42-110o	Attorney General: Conn. Gen. Stat. §§ 36a-701b(g), 42-110o

Connecticut Personal Information Protection Act	Conn. Gen. Stat. § 42-471	"Any person who collects Social Security numbers in the course of business shall create a privacy protection policy which shall be published or publicly displayed. For purposes of this subsection, "publicly displayed" includes, but is not limited to, posting on an Internet web page. Such policy shall: (1) Protect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers."	Up to $5,000 per violation: Conn. Gen. Stat. §§ 42-471(h), 36a-701b(g), 42-110o,	Attorney General: Conn. Gen. Stat. §§ 42-471(h), 36a-701b(g), 42-110o,
Connecticut Unfair, Deceptive, or Abusive Acts and Practices	Conn. Gen. Stat. § 42-110b	"No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."	Up to $5,000 per violation: Conn. Gen. Stat. § 42-110o	Attorney General: Conn. Gen. Stat. § 42-110o
Delaware Breach Notification Law	Del. Code tit. 6, § 12B-102	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay, but no more than 60 days • Substitute Notice: Yes, if over 100,000 residents or $75,000 • Credit Monitoring: Yes, if SSN breached, 12 months • Other:	"an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both." 6 Del. C. § 12B-104	Director of Consumer Protection of the Department of Justice: 6 Del. C. § 12B-104
Delaware Personal Information Protection Act	Del. Code tit. 6, § 12B-100	"Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business."	"an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both." 6 Del. C. § 12B-104	Director of Consumer Protection of the Department of Justice: 6 Del. C. § 12B-104
Delaware Unfair, Deceptive, or Abusive Acts and Practices	Del. Code tit. 6, § 2532	"A person engages in a deceptive trade practice when, in the course of a business, vocation, or occupation, that person:. . ."	Up to $10,000 per willful violation: Del. Code tit. 6, § 2533	Attorney General: Del. Code tit. 6, § 2533
Florida Breach Notification Law	Fla. Stat. § 501.171(4)(a)	• Notify Affected Residents: Yes • Notify Department of Legal Affairs: Yes, if over 500 • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 500,000 residents or $250,000 • Credit Monitoring: • Other:	Up to $500,000 and more penalties: Fla. Stat. § 501.171(9)	Department of Legal Affairs: Fla. Stat. § 501.171(9)
Personal Information Protection Act	Fla. Stat. § 501.171(2)	"Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information."	Up to $500,000 and more penalties: Fla. Stat. § 501.171(9)	Department of Legal Affairs: Fla. Stat. § 501.171(9)
Unfair, Deceptive, or Abusive Acts and Practices	Fla. Stat. § 501.204	"Unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful"	Up to $10,000 per violation: Fla. Stat. § 501.2075	Department of Legal Affairs: Fla. Stat. § 501.2075
Georgia Breach Notification Law	Ga. Code § 10-1-912	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 10,000 residents • If not data owner, notify data owner: Yes, within 24 hours • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 100,000 residents or $50,000 • Credit Monitoring: No	None	None
Unfair, Deceptive, or Abusive Acts and Practices	Ga. Code § 10-1-393	"Unfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce are declared unlawful."	Up to $5,000 per violation: Ga. Code § 10-1-397(a)(2)(B)	Attorney General: Ga. Code § 10-1-397

Hawaii Breach Notification Law	Haw. Rev. Stat. § 487N-2	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 200,000 residents or $100,000 • Credit Monitoring: No	Up to $2,500 per violation: Haw. Rev. Stat. § 487N-3	Attorney General: Haw. Rev. Stat. § 487N-3
Unfair, Deceptive, or Abusive Acts and Practices	Haw. Rev. Stat. § 480-2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful."	Up to $10,000 per violation: Haw. Rev. Stat. § 480-3.1	Attorney General or Director of the Office of Consumer Protections: :Haw. Rev. Stat. § 480-3.1
Idaho Breach Notification Law	Idaho Code § 28-51-105	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $25,000 • Credit Monitoring: No	Up to $25,000 per breach: Idaho Code § 28-51-107	Attorney General: Idaho Code § 28-51-107
Unfair, Deceptive, or Abusive Acts and Practices	Idaho Code § 48-603	"The following unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared to be unlawful, where a person knows, or in the exercise of due care should know, that he has in the past, or is:"	Up to $10,000 per violation: Idaho Code § 48-606(1)(e)	Attorney General: Idaho Code § 48-606
Illinois Breach Notification Law	815 Ill. Comp. Stat. § 530/10	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Up to $50,000: 815 ILCS §§ 530/20; 505/7	Attorney General: 815 ILCS §§ 530/20; 505/7
Personal Information Protection Act	815 Ill. Comp. Stat. § 530/45	"A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."	Up to $50,000: 815 ILCS §§ 530/20; 505/7	Attorney General: 815 ILCS §§ 530/20; 505/7
Unfair, Deceptive, or Abusive Acts and Practices	815 Ill. Comp. Stat. § 505/2	"Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in Section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965,1 in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a) of the Federal Trade Commission Act.2"	Up to $50,000: 815 Ill. Comp. Stat. § 505/7	Attorney General: 815 Ill. Comp. Stat. § 505/7
Iowa Breach Notification Law	Iowa Code § 715C.2	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 350,000 residents or $250,000 • Credit Monitoring: No	Up to $40,000 per violation: Iowa Code §§ 715C.2(9), 714.16(7)	Attorney General: Iowa Code §§ 715C.2(9), 714.16(7)

Unfair, Deceptive, or Abusive Acts and Practices	Iowa Code § 714.16	"The act, use or employment by a person of an unfair practice, deception, fraud, false pretense, false promise, or misrepresentation, or the concealment, suppression, or omission of a material fact with intent that others rely upon the concealment, suppression, or omission, in connection with the lease, sale, or advertisement of any merchandise or the solicitation of contributions for charitable purposes, whether or not a person has in fact been misled, deceived, or damaged, is an unlawful practice."	Up to $40,000 per violation: Iowa Code § 714.16(7)	Attorney General: Iowa Code § 714.16(7)
Kansas Breach Notification Law	Kan. Stat. § 50-7a02	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $100,000 • Credit Monitoring: No	"an action in law or equity to address violations of this section and for other relief that may be appropriate": Kan. Stat. § 50-7a02(g)	Attorney General: Kan. Stat. § 50-7a02(g)
Personal Information Protection Act	Kan. Stat. § 50-6,139b(b)(1)	" A holder of personal information shall: (1) Implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure. If federal or state law or regulation governs the procedures and practices of the holder of personal information for such protection of personal information, then compliance with such federal or state law or regulation shall be deemed compliance with this paragraph and failure to comply with such federal or state law or regulation shall be prima facie evidence of a violation of this paragraph; . . ."	Up to $10,000 per violation or $20,000 per willful violation: Kan. Stat. §§ 50-6139b(d, e), 50-636	Attorney General: Kan. Stat. § 50-636
Unfair, Deceptive, or Abusive Acts and Practices	Kan. Stat. § 50-626	"No supplier shall engage in any deceptive act or practice in connection with a consumer transaction."	Up to $10,000 per violation or $20,000 per willful violation: Kan. Stat. § 50-636	Attorney General: Kan. Stat. § 50-636
Kentucky Breach Notification Law	Ky. Rev. Stat. § 365.732	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: • Other:	None	Private Right of Action: Ky. Rev. Stat. § 365.730
Unfair, Deceptive, or Abusive Acts and Practices	Ky. Rev. Stat. § 367.170	"Unfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $2,000 per violation: Ky. Rev. Stat. § 367.990(2)	Attorney General: Ky. Rev. Stat. § 367.990(2)
Louisiana Breach Notification Law	La. Rev. Stat. § 51:3074	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $250,000 • Credit Monitoring: No • Other:	"a fine not to exceed $5,000 per violation. Notice to the attorney general shall be timely if received within 10 days of distribution of notice to Louisiana citizens. Each day notice is not received by the attorney general shall be deemed a separate violation." 16 La. Admin. Code Pt III, 701	Attorney General: 16 La. Admin. Code Pt III, 701
Unfair, Deceptive, or Abusive Acts and Practices	La. Stat. § 51:1405	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: La. Rev. Stat. § 51:1407(B)	Attorney General: La. Rev. Stat. § 51:1407(A)

Maine Breach Notification Law	Me. Rev. Stat. tit. 10 § 1348	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 1,000 people or $5,000 • Credit Monitoring: No	"[M]aximum of $2,500 for each day the person is in violation:" Me. Rev. Stat. tit. 10 § 1349	Attorney General: Me. Rev. Stat. tit. 10 § 1349
Unfair, Deceptive, or Abusive Acts and Practices	Me. Rev. Stat. tit. 5 § 207	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are declared unlawful."	$5,000 penalty for non-compliance with § 211: Me. Rev. Stat. tit. 5 § 212	Attorney General: Me. Rev. Stat. tit. 5 § 212
Maryland Breach Notification Law	Md. Code, Com. Law § 14-3504	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, over 1000 • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay and several day requirements • Substitute Notice: Yes, if over 175,000 residents or $100,000 • Credit Monitoring: No • Other:	$1,000 per violation: Md. Code, Com. Law §§ 14-3508, 13-410	Division of Consumer Protection: Md. Code Comm . Law §§ 13-403 and 13-410
Personal Information Protection Act	Md. Code, Com. Law § 14-3503	"To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."	$1,000 per violation: Md. Code, Com. Law §§ 14-3508, 13-410	Division of Consumer Protection: Md. Code Comm . Law §§ 13-403 and 13-410
Unfair, Deceptive, or Abusive Acts and Practices	Md. Code Comm . Law §13-303	"A person may not engage in any unfair or deceptive trade practice, as defined in this subtitle or as further defined by the Division, in:. . ."	$1,000 per violation: Md. Code, Com. Law § 13-410	Division of Consumer Protection: Md. Code Comm . Law §§ 13-403 and 13-410
Massachusetts Breach Notification Law	Mass. Gen. Laws Ch. 93H § 1	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Attorney General • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,00 residents or $250,000 • Credit Monitoring: 2 years	Up to $5,000 per violation: Mass. Gen. Laws Ch. 93A § 4	Attorney General: Mass. Gen. Laws § 93H § 1
Unfair, Deceptive, or Abusive Acts and Practices	Mass. Gen. Laws Ch. 93A § 2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: Mass. Gen. Laws Ch. 93A § 4	Attorney General: Mass. Gen. Laws Ch. 93A § 4
Michigan Breach Notification Law	Mich. Comp. Laws § 445.72	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	$250 per notice failure, or up to $750,000 per breach: Mich. Comp. Laws § 445.72(13)	Attorney General: Mich. Comp. Laws § 445.72(13)
Unfair, Deceptive, or Abusive Acts and Practices	Mich. Comp. Laws § 445.903	"Unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce are unlawful and are defined as follows:. . ."	Up to $25,000: Mich. Comp. Laws § 445.905	Attorney General: Mich. Comp. Laws § 445.905

Minnesota Breach Notification Law	Minn. Stat. § 325E.61,	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 500 residents. Notification in 48 hours. • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Unclear: Minn. Stat. §§ 325E.61(6), 8.31	Attorney General: Minn. Stat. §§ 325E.61(6), 8.31
Unfair, Deceptive, or Abusive Acts and Practices	Minn. Stat. § 325F.69	"Fraud, misrepresentation, deceptive practices. The act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoinable as provided in section 325F.70."	Unclear: Minn. Stat. § 8.31	Attorney General: Minn. Stat. § 8.31
Mississippi Breach Notification Law	Miss. Code § 75-24-29	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $5,000 • Credit Monitoring: • Other:	$10,000 per violation: Miss. Code § 75-24-19	Attorney General: Miss. Code § 75-24-29(8)
Unfair, Deceptive, or Abusive Acts and Practices	Miss. Code § 75-24-5	"Unfair methods of competition affecting commerce and unfair or deceptive trade practices in or affecting commerce are prohibited. Action may be brought under Section 75-24-5(1) only under the provisions of Section 75-24-9."	$10,000 per violation: Miss. Code § 75-24-19	Attorney General: Miss. Code § 75-24-9
Missouri Breach Notification Law	Mo. Rev. Stat. § 407.1500	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 150,000 residents or $150,000 • Credit Monitoring: • Other:	Up to $150,000: Mo. Rev. Stat. § 407.1500(3)	Attorney General: Mo. Rev. Stat. § 407.1500(3)
Unfair, Deceptive, or Abusive Acts and Practices	Mo. Rev. Stat. § 407.020	"he act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce or the solicitation of any funds for any charitable purpose, as defined in section 407.453, in or from the state of Missouri, is declared to be an unlawful practice."	Up to $1000 per violation: Mo. Rev. Stat. § 407.100(6)	Attorney General: Mo. Rev. Stat. § 407.100
Montana Breach Notification Law	Mont. Code § 30-14-1704	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, coordination provision • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: • Other:	Up to $10,000 per willful violation: Mont. Code §§ 30-14-1705; 30-14-142(2)	Department of Justice (Attorney General): Mont. Code § 30-14-1705
Unfair, Deceptive, or Abusive Acts and Practices	Mont. Code § 30-14-103	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful."	Up to $10,000 per willful violation: Mont. Code § 30-14-142(2)	Department of Justice (Attorney General): Mont. Code § 30-14-1705

Nebraska Breach Notification Law	Nebraska Neb. Rev. Stat. § 87-803	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $75,000 • Credit Monitoring: No	Direct economic damage: Neb. Rev. Stat. § 87-806	Attorney General: Neb. Rev. Stat. § 87-806
Unfair, Deceptive, or Abusive Acts and Practices	Neb. Rev. Stat. § 59-1602	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce shall be unlawful."	Up to $2,000 per violation: Neb. Rev. Stat. § 59-1614	Attorney General: Neb. Rev. Stat. § 59-1614
Nevada Breach Notification Law	Nev. Rev. Stat. § 603A.220	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Injunction: Nev. Rev. Stat. § 603A.290	Attorney General: Nev. Rev. Stat. § 603A.290
Personal Information Protection Act	Nev. Rev. Stat. § 603A.210	"A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."	Injunction: Nev. Rev. Stat. § 603A.290	Attorney General: Nev. Rev. Stat. § 603A.290
Unfair, Deceptive, or Abusive Acts and Practices	Neb. Rev. Stat. § 59-1602	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce shall be unlawful."	Up to $2,000 per violation: Neb. Rev. Stat. § 59-1614	Attorney General: Neb. Rev. Stat. § 59-1608
New Hampshire Breach Notification Law	N.H. Rev. Stat. § 359-C:20	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if subject to N.H. Rev. Stat. § 358-A:3(I) • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: As soon as possible • Substitute Notice: Yes, if over 1,000 residents or $5,000 • Credit Monitoring: No	Up to $10,000 per violation: N.H. Rev. Stat. §§ 359-C:20; 358-A:4(III)(b)	Attorney General: N.H. Rev. Stat. §§ 359-C:20; 358-A:4
Unfair, Deceptive, or Abusive Acts and Practices	N.H. Rev. Stat. § 358-A:2	"It shall be unlawful for any person to use any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state. Such unfair method of competition or unfair or deceptive act or practice shall include, but is not limited to, the following:"	Up to $10,000 per violation: N.H. Rev. Stat. § 358-A:4(III)(b)	Consumer Protection and Antitrust Bureau, Department of Justice: N.H. Rev. Stat. § 358-A:4
New Jersey Breach Notification Law	N.J. Stat. § 56:8-163	• Notify Affected Residents: Yes • Notify Attorney General: Yes, prior to notification to customers • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No • Other:	Up to $10,000 for the first offense, and $20,000 for subsequent offenses: N.J. Stat. § 56:8-13	Attorney General: N.J. Stat. § 56:8-3.1

Unfair, Deceptive, or Abusive Acts and Practices	N.J. Stat. § 56:8-2	"The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice; provided, however, that nothing herein contained shall apply to the owner or publisher of newspapers, magazines, publications or printed matter wherein such advertisement appears, or to the owner or operator of a radio or television station which disseminates such advertisement when the owner, publisher, or operator has no knowledge of the intent, design or purpose of the advertiser."	Up to $10,000 for the first offense, and $20,000 for subsequent offenses: N.J. Stat. § 56:8-13	Attorney General: N.J. Stat. § 56:8-3.1
New Mexico Breach Notification Law	N.M. Stat. § 57-12c-6	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: No later than 45 days after the breach discovery date • Substitute Notice: Yes, if over 50,000 residents or $100,000 • Credit Monitoring: No	Up to $150,000: N.M. Stat. § 57-12c-11	Attorney General: N.M. Stat. § 57-12c-11
Personal Information Protection Act	N.M. Stat. § 57-12c-4	"A person that owns or licenses personal identifying information of a New Mexico resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure."	Up to $25,000: N.M. Stat. § 57-12c-11	Attorney General: N.M. Stat. § 57-12c-11
Unfair, Deceptive, or Abusive Acts and Practices	N.M. Stat. § 57-12-3	"Unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce are unlawful."	Up to $5,000 per violation: N.M. Stat. § 57-12-11	Attorney General: N.M. Stat. § 57-12-11
New York Breach Notification Law	N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 5000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Up to $150,000: N.Y. Gen. Bus. Law § 899-AA(6)	Attorney General: N.Y. Gen. Bus. Law § 899-AA(6)
Unfair, Deceptive, or Abusive Acts and Practices	N.Y. Gen. Bus. Law § 349	"Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."	Up to $5,000 per violation: N.Y. Gen. Bus. Law § 350-d	Attorney General: N.Y. Gen. Bus. Law § 349(f)
North Carolina Breach Notification Law	N.C. Gen. Stat § 75-65	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 or $250,000 • Credit Monitoring: No • Other:	Up to $5,000 per violation: N.C. Gen. Stat. §§ 75-65(i), 75-15.2	Attorney General: N.C. Gen. Stat. §§ 75-65(i), 75-15
Unfair, Deceptive, or Abusive Acts and Practices	N.C. Gen. Stat. § 75-1.1	"Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful."	Up to $5,000 per violation: N.C. Gen. Stat. § 75-15.2	Attorney General: N.C. Gen. Stat. § 75-15

North Dakota Breach Notification Law	N.D. Cent. Code § 51-30-02	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 people • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 or $250,000 • Credit Monitoring: No	Up to $5,000 per violation: N.D. Cent. Code §§ 51-30-07, 51-15-11	Attorney General: N.D. Cent. Code § 51-30-07
Unfair, Deceptive, or Abusive Acts and Practices	N.D. Century Code § 51-15-02	"The act, use, or employment by any person of any deceptive act or practice, fraud, false pretense, false promise, or misrepresentation, with the intent that others rely thereon in connection with the sale or advertisement of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is declared to be an unlawful practice. The act, use, or employment by any person of any act or practice, in connection with the sale or advertisement of any merchandise, which is unconscionable or which causes or is likely to cause substantial injury to a person which is not reasonably avoidable by the injured person and not outweighed by countervailing benefits to consumers or to competition, is declared to be an unlawful practice."	Up to $5,000 per violation: N.D. Cent. Code § 51-15-11	Attorney General: N.D. Cent. Code § 51-15-07
Ohio Breach Notification Law	Ohio Rev. Code § 1349.19	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: No longer than 45 days following the breach discovery date • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No • Other: Substitute notice exception for small businesses.	Cascading penalties based on delay: Ohio Rev. Code § 1349.192	Attorney General: Ohio Rev. Code § 1349.19(i)
Unfair, Deceptive, or Abusive Acts and Practices	Ohio Rev. Code § 1345.02	"No supplier shall commit an unfair or deceptive act or practice in connection with a consumer transaction. Such an unfair or deceptive act or practice by a supplier violates this section whether it occurs before, during, or after the transaction."	Up to $25,000: Ohio Rev. Code § 1345.07	Attorney General: Ohio Rev. Code § 1345.02(E)(3)
Oklahoma Breach Notification Law	Okla. Stat. tit. 24, § 163	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: No	Up to $150,000: Okla. Stat. § 24-165	Attorney General: Okla. Stat. § 24-165
Unfair, Deceptive, or Abusive Acts and Practices	Okla. Stat. tit. 15, § 753	"A person engages in a practice which is declared to be unlawful under the Oklahoma Consumer Protection Act when, in the course of the person's business, the person . . ."	Up to $2,000 per violation or up to $10,000 per willful violation: Okla. Stat. tit. 15, § 761.1	Attorney General: Okla. Stat. tit. 15, § 761.
Oregon Breach Notification Law	Oregon Rev. Stat. § 646A.604	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 350,000 residents and $250,000 • Credit Monitoring: Yes	Or. Rev. Stat. §§ 646A.604(9)(a), 646.642(3)	Director of the Department of Consumer and Business Services: Or. Rev. Stat. § 646A.624
Personal Information Protection Act	Or. Rev. Stat. § 646A.622	"A person that owns, maintains or otherwise possesses, or has control over or access to, data that includes personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information."	Up to $1000 per violation: Or. Rev. Stat. § 646A.624	Director of the Department of Consumer and Business Services: Or. Rev. Stat. § 646A.624

Unfair, Deceptive, or Abusive Acts and Practices	Or. Rev. Stat. § 646.607	"A person engages in an unlawful trade practice if in the course of the person's business, vocation or occupation the person. . ."	Up to $250,000 per violation: Or. Rev. Stat. § 646.642(3)	Prosecuting attorney: Or. Rev. Stat. § 646.642(3)
Pennsylvania Breach Notification Law	73 Pa. Stat. § 2303	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 175,000 people or $100,000 • Credit Monitoring: No	Up to $1,000 per violation: 73 Pa. Stat. §§ 2308, 201-8	Attorney General: 73 Pa. Stat. § 2308
Unfair, Deceptive, or Abusive Acts and Practices	73 Pa. Stat. § 201-3	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce as defined by subclauses (i) through (xxi) of clause (4) of section 21 of this act and regulations promulgated under section 3.12 of this act are hereby declared unlawful. The provisions of this act shall not apply to any owner, agent or employee of any radio or television station, or to any owner, publisher, printer, agent or employee of an Internet service provider or a newspaper or other publication, periodical or circular, who, in good faith and without knowledge of the falsity or deceptive character thereof, publishes, causes to be published or takes part in the publication of such advertisement."	Up to $1,000 per violation: 73 Pa. Stat. § 201-8	Attorney General: 73 Pa. Stat. § 201-8
Rhode Island Breach Notification Law	R.I. Gen. Laws § 11-49.3-4	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over • Credit Monitoring: • Other:	$100 per reckless violation, $200 per knowing/willful violation: R.I. Gen. Laws § 11-49.3-5	Attorney General: R.I. Gen. Laws § 11-49.3-5
Personal Information Protection Act	R.I. Gen. Laws § 11-49.3-2	"A municipal agency, state agency or person that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information. A municipal agency, state agency, or person shall not retain personal information for a period longer than is reasonably required to provide the services requested; to meet the purpose for which it was collected; or in accordance with a written retention policy or as may be required by law. A municipal agency, state agency, or person shall destroy all personal information, regardless of the medium that such information is in, in a secure manner, including, but not limited to, shredding, pulverization, incineration, or erasure."	$100 per reckless violation, $200 per knowing/willful violation: R.I. Gen. Laws § 11-49.3-5	Attorney General: R.I. Gen. Laws § 11-49.3-5
Unfair, Deceptive, or Abusive Acts and Practices	R.I. Gen. Laws § 6-13.1-2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are declared unlawful."	Up to $10,000 per violation: R.I. Gen. Laws § 6-13.1-8	Attorney General: R.I. Gen. Laws § 6-13.1-8
South Carolina Breach Notification Law	S.C. Code § 39-1-90	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over • Credit Monitoring: • Other:	$1,000 per resident for knowing or willful violation: S.C. Code § 39-1-90(H)	Attorney General: S.C. Code § 39-1-90(H)
Unfair, Deceptive, or Abusive Acts and Practices	S.C. Code § 39-5-20	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: S.C. Code § 39-5-110	Attorney General: S.C. Code § 39-5-110

South Dakota Breach Notification Law	SD SB62	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 residents • Notify Credit Reporting Agencies: Yes • If not data owner, notify data owner: Yes • How many days to Notify: Within 60 days of breach discovery date. • Substitute Notice: Yes, if over 500,000 people or $250,000 • Credit Monitoring: • Other:	Enacted on 3/21/2018, effective July 1, 2018	http://sdlegislature.gov/docs/legsession/2018/Bills/SB62ENR.pdf
Unfair, Deceptive, or Abusive Acts and Practices	S.D. Codified Laws § 37-24-6	"It is a deceptive act or practice for any person to: (1) Knowingly act, use, or employ any deceptive act or practice, fraud, false pretense, false promises, or misrepresentation or to conceal, suppress, or omit any material fact in connection with the sale or advertisement of any merchandise, regardless of whether any person has in fact been misled, deceived, or damaged thereby. . ."	Up to $2,000 per violation: S.D. Codified Laws § 37-24-27	Attorney General: S.D. Codified Laws § 37-24-23
Tennessee Breach Notification Law	Tenn. Code § 47-18-2107	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes, within 45 of breach discovery date • How many days to Notify: Within 45 of breach discovery date • Substitute Notice: Yes, if over 500,000 people or $250,000 • Credit Monitoring: No	"civil penalty of whichever of the following is greater: ten thousand dollars ($10,000), five thousand dollars ($5,000) per day for each day that a person's identity has been assumed or ten (10) times the amount obtained or attempted to be obtained by the person using the identity theft.": Tenn. Code § 47-18-2105	Division of Consumer Affairs of the Department of Commerce and Insurance: Tenn. Code § 47-18-2105
Personal Information Protection Act	Tenn. Code § 47-18-2110	"On and after January 1, 2008, any person, nonprofit or for profit business entity in this state, including, but not limited to, any sole proprietorship, partnership, limited liability company, or corporation, engaged in any business, including, but not limited to, health care, that has obtained a federal social security number for a legitimate business or governmental purpose shall make reasonable efforts to protect that social security number from disclosure to the public."	"civil penalty of whichever of the following is greater: ten thousand dollars ($10,000), five thousand dollars ($5,000) per day for each day that a person's identity has been assumed or ten (10) times the amount obtained or attempted to be obtained by the person using the identity theft.": Tenn. Code § 47-18-2105	Division of Consumer Affairs of the Department of Commerce and Insurance: Tenn. Code § 47-18-2105
Unfair, Deceptive, or Abusive Acts and Practices	Tenn. Code § 47-18-104	The following unfair or deceptive acts or practices affecting the conduct of any trade or commerce are declared to be unlawful and in violation of this part:	Up to $1,000 per violation: Tenn. Code § 47-18-108(b)(3)	Division of Consumer Affairs of the Department of Commerce and Insurance: Tenn. Code § 47-18-108
Texas Breach Notification Law	Tex. Bus. & Com. Code § 521.053	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 10,000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 people or $250,000 • Credit Monitoring: No	Between $2,000 and $50,000 per violation and up to $150,000 in additional penalties: Tex. Bus. & Com. Code § 521.151	Attorney General: Tex. Bus. & Com. Code § 521.151
Personal Information Protection Act	Tex. Bus. & Com. Code § 521.052	"A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business."	Between $2,000 and $50,000 per violation: Tex. Bus. & Com. Code § 521.151	Attorney General: Tex. Bus. & Com. Code § 521.151
Unfair, Deceptive, or Abusive Acts and Practices	Tex. Bus. & Com. Code § 17.45	"False, misleading, or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful and are subject to action by the consumer protection division. . ."	Up to $20,000 per violation: Tex. Bus. & Com. Code § 17.47	Consumer Protection Division, Attorney General: Tex. Bus. & Com. Code § 17.47

Utah Breach Notification Law	Utah Code § 13-44-202	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Not allowed • Credit Monitoring: No	Up to $100,000: Utah Code § 13-44-301	Attorney General: Utah Code § 13-44-301
Personal Information Protection Act	Utah Code § 13-44-201	"Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person."	Up to $100,000: Utah Code § 13-44-301	Attorney General: Utah Code § 13-44-301
Unfair, Deceptive, or Abusive Acts and Practices	Utah Code § 13-11-5	"An unconscionable act or practice by a supplier in connection with a consumer transaction violates this act1 whether it occurs before, during, or after the transaction."	Up to $2,500 per violation (administrative fine): Utah Code § 13-11-17	Division of Consumer Protections: Utah Code § 13-11-17
Vermont Breach Notification Law	Vt. Stat. tit. 9 § 2435	• Notify Affected Residents: Yes • Notify Attorney General: Yes, within 14 business days of breach discovery • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $5,000 • Credit Monitoring: • Other:	Unclear from statute	Attorney General: Vt. Stat. tit. 9 § 2435(g)
Unfair, Deceptive, or Abusive Acts and Practices	Vt. Stat. tit. 9, § 2453	"Unfair methods of competition in commerce and unfair or deceptive acts or practices in commerce are hereby declared unlawful."	Up to $10,000 per violation: Vt. Stat. tit. 9, § 2461	Attorney General: Vt. Stat. tit. 9, § 2461
Virginia Breach Notification Law	Va. Code § 18.2-186.6	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: • Other: Special provisions for income tax data	Up to $150,000 per breach: Va. Code § 18.2-186.6(I)	Attorney General: Va. Code § 18.2-186.6(I)
Unfair, Deceptive, or Abusive Acts and Practices	Va. Code § 59.1-200	"The following fraudulent acts or practices committed by a supplier in connection with a consumer transaction are hereby declared unlawful . . ."	Up to $2,500 per violation: Va. Code § 59.1-206	Attorney General: Va. Code § 59.1-206
Washington Breach Notification Law	Wash. Rev. Code § 19.255.010	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: No more than 45 days after the breach discovery • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: • Other: Reimbursement from businesses to financial institutions provision	Up to $25,000: Wash. Rev. Code §§ 19.255.010(17), 19.86.140	Attorney General: Wash. Rev. Code § 19.255.010(17)
Unfair, Deceptive, or Abusive Acts and Practices	Wash. Rev. Code § 19.86.020	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $25,000: Wash. Rev. Code § 19.86.140	Attorney General: Wash. Rev. Code § 19.86.080

West Virginia Breach Notification Law	W.Va. Code § 46A-2A-102	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: No • Other:	Up to $5,000 per violation: W.Va. Code §§ 46A-2A-104, 46A-7-111	Attorney General: W.Va. Code § 46A-2A-104
Unfair, Deceptive, or Abusive Acts and Practices	W. Va. Code § 46A-6-104	Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: W.Va. Code § 46A-7-111	Attorney General: W.Va. Code § 46A-7-111
Wisconsin Breach Notification Law	Wis. Stat. § 134.98	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Within 45 days of the breach discovery date • Substitute Notice: Yes, see statute • Credit Monitoring:	None	No one
Unfair, Deceptive, or Abusive Acts and Practices	Wis. Stat. § 100.20	"Methods of competition in business and trade practices in business shall be fair. Unfair methods of competition in business and unfair trade practices in business are hereby prohibited."	From $100 to $10,000 per violation: Wis. Stat. § 100.26(6)	The Department of Agriculture, trade, and consumer protection: Wis. Stat. § 100.20
Wyoming Breach Notification Law	Wyo. Stat. § 40-12-502	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, see statute • Credit Monitoring: No	Damages: Wyo. Stat. § 40-12-502	Attorney General: Wyo. Stat. § 40-12-502(f)
Unfair, Deceptive, or Abusive Acts and Practices	Wyo. Stat. § 40-12-105	"A person engages in a deceptive trade practice unlawful under this act when, in the course of his business and in connection with a consumer transaction, he knowingly. . ."	Up to $5,000 per violation: Wyo. Stat. § 40-12-113	Attorney General: Wyo. Stat. § 40-12-113
District of Columbia Breach Notification Law	D.C. Code § 28- 3852	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 or $50,000 • Credit Monitoring: No	$100 per Affected Resident: D.C. Code § 28- 3853	US Attorney General: D.C. Code § 28- 3853
Unfair, Deceptive, or Abusive Acts and Practices	D.C. Code § 28-3904	"It shall be a violation of this chapter, whether or not any consumer is in fact misled, deceived or damaged thereby, for any person to: . . ."	Up to $1000 per violation: D.C. Code § 28-3909	Corporation Counsel: D.C. Code § 28-3909
Guam Breach Notification Law	9 GCA § 48.30	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $10,000 • Credit Monitoring: No • Other:	Up to $150,000 per breach: 9 GCA § 48.50	The Attorney General: 9 GCA § 48.50

Unfair, Deceptive, or Abusive Acts and Practices	5 GCA § 32201	"False, misleading, or deceptive acts or practices, including, but not limited to those listed in this chapter, are hereby declared unlawful and are subject to action by the Attorney General or any person as permitted pursuant to this chapter or other provisions of Guam law. A violation consisting of any act prohibited by this title is in itself actionable, and may be the basis for damages, rescission, or equitable relief. The provisions of this chapter are to be liberally construed in favor of the consumer, balanced with substantial justice, and violation of such provisions may be raised as a claim, defense, crossclaim or counterclaim."	Up to $5,000 per violation: 5 GCA § 32127	Attorney General: 5 GCA § 32116
Puerto Rico Breach Notification Law	10 Laws of Puerto Rico § 4051	• Notify Affected Residents: Yes • Notify the Secretary of Consumer Affairs: Yes, within 10 days • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 people or $100,000 • Credit Monitoring: No	Up to $5,000 per violation of the provisions of this chapter: 10 Laws of Puerto Rico § 4055	The Secretary: 10 Laws of Puerto Rico § 4055
Unfair, Deceptive, or Abusive Acts and Practices	10 Laws of Puerto Rico § 259	"Unfair methods of competition, and unfair or deceptive acts or practices in trade or commerce are hereby declared unlawful."	"a civil penalty imposed by the Department of Consumer Affairs up to a maximum of five thousand dollars ($5,000). Each separate violation of said decision shall be considered as continuous noncompliance therewith, in which case, each day the decision is not complied with shall be considered as a separate violation." 10 Laws of Puerto Rico § 259	The Office of Monopolistic Affairs: 10 Laws of Puerto Rico § 259
Virgin Islands Breach Notification Law	V.I. Code tit. 14, § 2208	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $100,000 • Credit Monitoring: No • Other:	Actual damages: V.I. Code tit. 14, § 2211	Private right of action: V.I. Code tit. 14, § 2211
Unfair, Deceptive, or Abusive Acts and Practices	V.I. Code tit. 12, § 101	"No person shall engage in any deceptive or unconscionable trade practice in the sale, lease, rental or loan or in the offering for sale, lease, rental, or loan of any consumer goods or services, or in the collection of consumer debts."	Up to $5,000 per violation: V.I. Code tit. 12, § 104	The Commissioner: V.I. Code tit. 12, § 104

Survey of International Cyber Laws

Title	Country	Information	Applies to	Notes
China Cybersecurity Law (CSL)	CHINA	CSL regulates the construction, operation, maintenance and use of networks, as well as network security supervision and management within mainland China. The Cyberspace Administration of China (CAC) is the primary governmental authority supervising and enforcing the CSL.		
General Data Privacy Regulation (GDPR)	EUROPEAN UNION	The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.	Countries that belong to the EEA include EU + 3. Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom. Non-EU countries in the EEA Norway, Iceland, Liechtenstein	While GDPR is In place as law there is not yet specific country by country adoption of laws to align or go stricter than GDPR. It should be expected that Germany, France and Spain will go above and beyond the standard GDPR language and add more provisions.
International Traffic in Arms Regulations (ITAR)	UNITED STATES	A United States regulatory regime to restrict and control the export of defense and military related technologies to safeguard U.S. national security and further U.S. foreign policy objectives ITAR is the International Traffic in Arms Regulations and requires, in part, that defense-related articles and technical data listed on the United States Munitions List USML only be shared with U.S. citizens absent special authorization or exemption. Furthermore, ITAR is a set of standards that deals with information security involving any parties that handle technical data related to the manufacturing, the exporting and a general involvement with defense articles or services.		
Encryption and Export Administration Regulation (EAR)		The Export Administration Regulations (EAR) is a set of US government regulations on the export and import of most commercial items. The U.S. Department of Commerce is responsible for implementing and enforcing EAR. Specifically, working with items deemed dual-use and having both commercial and military applications. In particular, encryption or Cryptographic Information Security		
Australia		The Privacy Act includes thirteen Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information (including sensitive information).		
India	India	India is not a part of any convention on protection of personal data that is equvalent to the GDPR. India has adopted other international declarations and conventions including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, these acts recognise the right to privacy.		
Japan		European Union (EU)-Japan Economic Partnership Agreement (EPA) is a reciprocal adequacy arrangement that established the equivalence of the EU's General Data Protection Regulation (GDPR) and Japan's Act on the Protection of Personal Information (APPI) and enabling cross-border data transfers between the two. Japan was previously not included in the EU's whitelist of countries considered as having adequate levels of personal data protection.		

Russia		In 2014, Russia adopted personal data localisation rules. These rules required all operators that collect and process Russian citizens personal data to use databases located in Russia. These requirements apply to the personal data of all Russian citizens, regardless of their relation with the company. The new rules do not cross-border transfer of personal data. However, the requirement for primary data processing via Russian databases is considered to be onerous.		
Canada		Canada has adequacy with the EU and GDPR (as of the launch of GDPR) based on the PIPDEA law that covers data privacy in Canada. In general, Canada privacy is not that bad. However, organizations in British Columbia and Nova Scotia that do business with quasi-governmental entities such as banks & transportation are subject to FIPPA. In particualr, article 30. is critical to understand as it prohibits transfer of data outside of Canada.		

Survey of Institutions

Title	Information	URL
Cloud Security Alliance	Offers a number of certifications including: CSA Security, Trust & Assurance Registry (STAR) Certificate of Cloud Security Knowledge (CCSK) Certified Cloud Security Professional (CCSP) Global Consultancy Program	https://cloudsecurityalliance.org/
Commission on Accreditation for Law Enforcement Agencies ("CALEA")	CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance while protecting the privacy of information outside the scope of the investigation. It requires that telecommunications carriers and manufacturers of telecommunications equipment design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for information.	http://www.calea.org/
Control Objectives for Information and Related Technologies ("COBIT")	COBIT 5 is the only business framework for the governance and management of enterprise IT. COBIT 5 integrates other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®) and related standards from the International Organization for Standardization (ISO).	http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
Federal Energy Regulatory Commission (FERC) Revised Critical Infrastructure Protection (CIP) Reliability Standards	NERC, which FERC has certified as the nation's Electric Reliability Organization, developed Critical Infrastructure Protection (CIP) cyber security reliability standards. On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards, while concurrently directing NERC to develop significant modifications addressing specific concerns. In January 2016, FERC issued a Final Rule revising the CIP reliability standards. Docket No. RM15-14-000. As of December 2017, FERC release a Notice of Proposed Rulemaking to direct NERC to develop and submit modifications to improve mandatory reporting of Cyber Security Incidents. [Docket Nos. RM18-2-000 and AD17-9-000.	https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp
Federal Financial Institutions Examination Councils ("FFIEC")	The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions. Guidance includes: Online Banking: https://www.ffiec.gov/pdf/authentication_guidance.pdf FFIEC Cybersecurity Assessment Tool: https://www.ffiec.gov/cyberassessmenttool.htm	https://www.ffiec.gov/
Health Insurance Trust Alliance (HITRUST) CSF	HITRUST CSF is a certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management.	https://hitrustalliance.net/hitrust-csf/

Indiana Department of Financial Institutions (DFI)	Enforces FFIEC standards.	https://www.in.gov/dfi/
Indiana State Insurance Commissioners Navigators and Application Organizations		https://www.in.gov/idoi/
International Organization for Standardization ("ISO")	ISO creates documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.	https://www.iso.org/home.html
ISA/IEC 62443 (ISA99)	The ISA-99/IEC 62443 standard is the worldwide standard for security of the Industrial Control Systems in the Operational Technology (OT) domain of organizations. The standard was created by the International Society of Automation, a leading worldwide nonprofit organization. The standard offers organizations handles to improve the digital security and safety of their process and SCADA environments.	https://www.isa.org/isa99/
National Institute of Standards and Technology ("NIST")	NIST is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce.	https://www.nist.gov/
North American Electric Reliability Corporation ("NERC")	The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel.	https://www.nerc.com/Pages/default.aspx
PCI Security Standards Council	Helps merchants and financial institutions understand and implement standards for security policies, technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data. Also helps vendors understand and implement standards for creating secure payment solutions.	https://www.pcisecuritystandards.org/
SSAE-18/ ISAE 3402	ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting.	https://www.ssae-16.com/soc-1-report/the-ssae-18-audit-standard/

APPENDIX D.16
LOCAL GOVERNMENT WORKING GROUP

LOCAL GOVERNMENT WORKING GROUP STRATEGIC PLAN

Chair: Rhonda Cook | Co-Chair: Stephanie Yager

September 2018
Indiana Executive Council on Cybersecurity

Local Government Working Group Plan

Contents

Committee Members **4**
Introduction **7**
Executive Summary **9**
Research **11**
Deliverable: Local Officials Cybersecurity Guidebook **14**
General information 14
Implementation Plan 15
Evaluation Methodology 19
Supporting Documentation **21**

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Rhonda Cook	Aim	Deputy Director	Chair / Full Time	Voting Proxy
Stephanie Yager	IACC	Executive Director	Co-Chair / Full Time	Voting Proxy
Debbie Driskell	Indiana Township Association	Executive Director	Full Time	Advisory
Mary Ferdon	City of Columbus	Exec Dir Admin /Community Development	Full Time	Advisory
James Haley	City of Fort Wayne	Director of IT	Full Time	Advisory
Ryan Hoff	AIC	Dir of Govt Affairs/General Counsel	Full Time	Advisory
Steve Luce	Indiana Sheriff's Assoc	Executive Director	As Needed	Contributing
Chris Mertens	Hamilton County	Director of IT	Full Time	Advisory
Doug Rapp	Rofori Corporation	President	As Needed	Advisory
Bill Wilson	Indiana Sheriff's Assoc	Jail Services Coordinator	Full Time	Contributing
Jodie Woods	Aim	General Counsel	Full Time	Advisory
Jay Phelps	Bartholomew County	Clerk	Full Time	Advisory
Mike Yoder	Elkhart County	Commissioner	As Needed	Voting
Matt Greller	Aim	Executive Director	As Needed	Voting
Tim Berry	Crowe Horwath	Managing Dir/Municipal Advisory Services	Full Time	Advisory
Krista Taggart	City of Greenwood	Corporation Counsel	Full Time	Advisory
Jon Weirick	City of Fort Wayne	Engineer / Utilities	As Needed	Advisory
Brad King	Indiana Election Commission	Director	As Needed	Advisory
Matthew Cloud	Ivy Tech	Project Director / Instructor / IT Dept	As Needed	Advisory
Beth Dlug	Allen County Elections Board	Director of Elections	Full Time	Advisory
Adam Krupp	Indiana Dept of Revenue	Commissioner	As Needed	Voting

Barry Ritter	Indiana Statewide 911 Board	Director	As Needed	Advisory
Jeff Roeder	Sondhi Solutions	Consultant	As Needed	Contributing
Will Dantzler	Sondhi Solutions	Consultant	As Needed	Contributing
Doug Kowalski	Indiana State Board of Accounts	Director of Legal Services	As Needed	Contributing
Jamie Palmer	IU Center for Urban Policy and the Environment	Planner/Policy Analyst	As Needed	Contributing
Alex Carroll	Lifeline Data Solutions	Consultant	As Needed	Contributing
Rich Banta	Lifeline Data Solutions	Consultant	As Needed	Advisory
Matthew Jacobson	Indiana State Board of Accounts	IT Manager	As Needed	Contributing
Dustin Balsar	Qumulus Solutions	Consultant	As Needed	Contributing
Christopher Larsen	City of Westfield	Director of Informatics	As Needed	Contributing
Timothy Renick	City of Carmel	Director of IT	As Needed	Contributing
Anahit Behjou	City of Bloomington	Legal Services	As Needed	Contributing
John B. Gregg	Aim	Grassroots Legislative Advocate	As Needed	Contributing

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - The Local Government Working Group met periodically over the course of the year to discuss the current status of local governments' capabilities to meet cybersecurity threats as well as the varying ways that some units are already addressing cybersecurity concerns. Survey data provided by the Indiana Advisory Commission on Intergovernmental Relations regarding cyber preparedness was reviewed by the committee. Insurance company applications for cyber coverage were also studied and reviewed. Input and examples from local officials, IT personnel and consultants also provided helpful background information.

- **Research Findings**
  - Ongoing end-user education is needed
  - Funding is needed to put internal controls in place and to fund consultants, insurance, software and hardware
  - Cooperative agreements and joint purchasing should occur to save money
    - Example: for the purchase of cyber insurance
  - Penetration testing and standardized assessment should be encouraged
  - Guidance is needed for choosing reputable vendors
  - Use of common terminology versus "industry jargon" is important
  - Local unit executive level officials are the best point of initial contact

- **Working Group Deliverable**
  - Local Officials Cybersecurity Guidebook

- **References**
  - National Institute of Standards and Technology (NIST): www.nist.gov
  - Indiana Advisory Commission on Intergovernmental Relations: www.iacir.spea.iupui.edu
  - Local Government Technology Association: www.igtla.org

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Local units have addressed the issue of cybersecurity at varying levels. Units with more resources have done more to educate, train and prepare for cybersecurity. Units with a full-time IT staff or access to greater resources are likely to have better protections.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Emergency services, record keeping, water and sewer operations.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Additional resources and funding.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Local units' emergency management plans are subject to approval by the Indiana Department of Homeland Security.
    b. Public record keeping and retention schedules are governed by state statute under the guidance of the Commission on Public Records.
    c. The State Board of Accounts oversees internal controls for local units.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. For local units that have engaged in penetration testing and exercises to gauge preparedness, these models would be helpful to other units that are ramping up their cybersecurity efforts.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. The deliverables were based on the knowledge and expertise of the members serving on the Local Government Working Group.
    b. Some resources that were cited and referred to over the course of our discussion include:
        - The Indiana Local Government Technology Association
        - National Network of Fusion Centers
        - MS-ISAC - Multi-state Information Sharing Analysis Center
        - NIST Cybersecurity Framework paper

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Education efforts are coordinated for local units in all states through groups such as the National League of Cities and the National Association of Counties. These groups host webinars, prepare articles and serve as a resource to their local membership.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Year one – awareness; Year three – funding, education, and initial protections; Year five – more advanced protections.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. A great deal of education is needed. Efforts to educate and raise awareness should be incorporated into regular training sessions and state called meetings. Making the discussion on cybersecurity easy to understand without tech jargon is important.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity, related workforce is not met?**
    a. The workforce of local units of government are locally elected officials and local government employees. A very small percentage of this workforce is cybersecurity related.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. Provide a funding mechanism so local units of government can employ additional resources and protections.

12. **What are your communication protocols in a cyber emergency?**
    a. Protocols would vary from local unit to local unit.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. Some best practices that have been identified include standardization of computerization, regular training sessions for employees, redundancy, and well-developed plans for addressing a cyberattack.

Deliverable: Local Officials Cybersecurity Guidebook

Deliverable: Local Officials Cybersecurity Guidebook

General information

1. **What is the deliverable?**
    a. The group's deliverable is a simplified guidebook written for local government executives to assist them in getting started with cybersecurity planning for their unit of government.

2. **What is the status of this deliverable?**
    a. In progress; 60% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. To provide education about the need for cybersecurity within local government and provide helpful resources.

6. **What metric or measurement will be used to define success?**
    a. Feedback and use of the materials.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Local government officials, local government, the citizens of Indiana.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Not certain.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Legal and water.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Office of Technology, Association of Indiana Counties, Accelerate Indiana Municipalities, Indiana Association of County Commissioners, Indiana Township Association.

12. **Who should be main lead of this deliverable?**
    a. Chairs of the local government working group in conjunction with its members.

13. **What are the expected challenges to completing this deliverable?**
    a. Simplifying complex technology jargon into common terms.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable (with periodic updates as needed)

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop a guidebook for local officials	Co-chairs Cook/Yager	60%	Fall 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
We would like to have available staff or outside consultants assist with the technical chapter on cyber-planning	N/A	Information technology technical expertise	State of Indiana	Grant or contribution	We have been told that there is no funding available to hire outside consultants for this task. IOT is checking on possible expertise that can assist us within state government.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Agreements from other associations to post the electronic guidebook on their websites	To make the information accessible to local officials.	Minimal				Existing staff within the associations should be able to post the materials on their websites

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Assistance provided to local officials.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. Hopefully, cybersecurity plans will be implemented at the local government level reducing the impact of threats. The cost to each local government is indeterminable and varies with size of government and current use of technology.

19. What is the risk or cost of not completing this deliverable?

a. Local officials with little resources will need to develop their own planning without the assistance of the guidebook.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. The feedback regarding the usefulness of the information in the guidebook will be the determination of its success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown
b. **If Yes, please list states/jurisdictions**
   i. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown
b. **If Yes, please list states/jurisdictions**
   i. Unknown.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Depending on the assistance we are able to secure for writing the cybersecurity planning chapter, this chapter will either be more developed or less developed.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
   i. However, the group would recommend that the State of Indiana take on the role of vetting vendors and consultants with which local governments may wish to contract. This is best done at the state level. We hope the state will run background checks, check that vendors are competent in what they do, and check to make sure that they are carrying proper liability insurance.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Very little support needed upon posting the information on the associations' websites; however, as new information evolves, it is foreseeable that the guidebook will require updating.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. IOT, Indiana Financial Authority (IFA), water group, and will be reaching out to the legal/insurance group.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. It would be applicable to both private and public sectors.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Local government officials will need to be made aware that the resource is available to them.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. We will work closely with the associations to get the word out about the guidebook. In addition, we foresee workshops and educational events at our conferences to continue education on the cybersecurity issue.

Evaluation Methodology

Objective 1: Develop a guidebook for local government officials to assist them with cybersecurity planning and education expected by fall of 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Promote guidebook on cybersecurity planning and education to local government officials throughout 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

No Supporting Documentation Provided At This Time

APPENDIX D.17

PERSONALLY IDENTIFIABLE INFORMATION WORKING GROUP

PERSONALLY IDENTIFIABLE INFORMATION WORKING GROUP STRATEGIC PLAN

Chair: Dewand Neely | Co-Chair: Valita Fredland

September 2018
Indiana Executive Council on Cybersecurity

Personally Identifiable Information Working Group Plan

Contents

Committee Members **4**

Introduction **6**

Executive Summary **8**

Research **12**

Deliverable: Indiana PII Guidebook **21**

General Information 21

Implementation Plan 23

Evaluation Methodology 27

Supporting Documentation **29**

Department of Revenue (DOR) PII Research Responses 30

State of Indiana Additional Terms and Conditions Software as a Service (SaaS) 34

State of Indiana Information Privacy Policy 42

Committee Members

Committee Members

Name	Organization	Title	Workgroup Position	IECC Membership Type
Dewand Neely	State of Indiana	Chief Information Officer	Chair	Voting
Ted Cotterill	State of Indiana	Chief Privacy Officer	Chair Proxy	Advisory
Valita Fredland	Indiana Health Information Exchange	VP – General Counsel & Privacy Officer	Co-Chair	Advisory
Doug Swetnam	Indiana Office of Attorney General	Section Chief – Data Privacy & Identify Theft Unit	Full Time	Voting Proxy
Tony Chu	Department of Revenue	Chief Information Security Officer	Full Time	Advisory
Mitch Parker	IU Health	Chief Information Security Officer	Full Time	Advisory
Leon Ravenna	KAR Auction Services	Chief Information Security Officer	Full Time	Advisory
Luke Britt	State of Indiana	Public Access Counselor	Full Time	Advisory
Ashley Schenck	Indiana Management Performance Hub	Director of Engagement & Analytics	Full Time	Advisory
Cliff McCullough	Family and Social Services Administration	Chief Privacy Officer	Full Time	Advisory
Chuck Cohen	Indiana Intelligence Fusion Center	Executive Director	Full Time	Voting Proxy
Dom Caristi	Ball State University	Professor of Telecommunications	Full Time	Advisory
Matt Odum	Briljent	President	Full Time	Advisory
Richard Braidich	RCR Technology	Chief Information Security Officer	Full Time	Advisory
John Lucas	Citizens Energy Group	VP of Information Technology	As Needed	Advisory
Lisa Berry-Tayman	CyberScout Solutions	Sr. Manager, Privacy and Information Guidance	Full Time	Advisory
Kim Metzger	Ice Miller	Partner	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Indiana Fair Information Practices Act, Ind. Code Ch. 4-1-6
    - http://iga.in.gov/legislative/laws/2017/ic/titles/004/#4-1-6
  - Indiana Access to Public Records Act, Ind. Code Ch. 5-14-3
    - http://iga.in.gov/legislative/laws/2017/ic/titles/005/#5-14-3
  - Indiana Disclosure of Security Breach Act, Ind. Code Art. 24-4.9
    - http://iga.in.gov/legislative/laws/2017/ic/titles/024/#24-4.9
  - Indiana Professional Services Contract Template
    - http://www.in.gov/idoa/files/Professional%20Services%20Contract%20Template%202017.docx
  - Indiana Additional Terms and Conditions, Software as a Service Engagements
  - State of Indiana Information Privacy Policy
  - NIST Privacy Program
    - https://www.nist.gov/privacy
  - NIST SP 800-53, Revision 5 (DRAFT), *Security and Privacy Controls for Information Systems and Organizations*
    - https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf
  - NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
    - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf
  - OMB Circular No. A-130 Revised
    - https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
  - OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
    - https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf
  - GAO Report, *Information Security: Protecting Personally Identifiable Information*
    - https://www.gao.gov/new.items/d08343.pdf
  - Privacy Act of 1974, 5 U.S.C. § 552a
    - https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf
  - E-Government Act of 2002
    - https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
  - FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*
    - https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
  - IAPP Glossary of Privacy Terms
    - https://iapp.org/resources/glossary/

- SANS CIS Critical Security Controls
  - https://www.sans.org/security-resources/posters/20-critical-security-controls/55/download

- **Research Findings**
  - The goal of defining "personally identifiable information" (PII) for use by a broad collection of individuals and entities presents a challenging task. This is due to the fact that there are many generally-applicable legal and policy definitions that include a similar set of data elements. For example, the State of Indiana's commercial data breach statute characterizes personal information as an unmasked social security number or first and last name with additional unmasked identifiers like a credit card number or driver's license number.[1] While this and similar PII characterizations are good candidates for use across multiple sectors, the US Office of Management and Budget defines PII as "…information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[2] This definition is particularly useful because it "…is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified."[3]
  - Laws like Children's Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), and their related administrative rules provide more specifically-applicable definitions which apply depending on the source of the information. Furthermore, certain acts provide de-identification methodologies that, if followed, allow the maintaining entity to make otherwise confidential information available publicly. One such example relates to the de-identification of protected health information. The rule allows for broader access to and use of the de-identified information if the following occurs:
    - A person with appropriate knowledge of and experience with generally accepted principles and methods for rendering information not individually identifiable… determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual…[4]
    - This rule acknowledges what is known as the "mosaic effect" whereby de-identified information can be combined with other available information to re-identify an individual. In this case, the definition of PII may be expanded to include other information that may be reasonably available to an anticipated recipient.

[1] Ind. Code § 24-4.9-2-10.
[2] OMB Memorandum M-07-16.
[3] GSA Policy and Procedure CIO P 2180.1.
[4] 45 CFR §164.514(b)(1).

- The current state of PII is one of change. The ability to re-identify an individual through the use of disparate, publicly-available datasets is real. As a result, the very definition of PII is in flux. A number of existing privacy regulations are cited above as "Research Conducted". While these are intended to protect the privacy of PII, many do so based upon possible historical use cases like the administration of a benefits program. Newer business intelligence technology offerings allow organizations to leverage information to make better-informed decisions and, while such use may fall within the spirit of these laws, there are few express allowances to be found. More and more, government is working to keep pace with emerging technologies, ensuring that the regulatory apparatus provides adequate protections to individuals while leaving room for innovation.
- To further complicate the matter, emerging technologies like Blockchain and related distributed ledger technologies have been discussed as potential solutions to the maintenance and exchange of high-value information. If applied to common PII maintenance and exchange scenarios, this decentralized maintenance of information presents such a significant departure from existing centralized models that related efforts would have to receive regulatory approval as pilot projects or run the risk of violating the law. In addition, there would need to be a shared governance model and auditing for distributed, decentralized systems to ensure integrity.

- **Final Deliverable**
  - Indiana PII Guidebook that will:
    - Define PII
    - Characterize the current state
    - Identify related regulations
    - Identify best practices across all sectors
    - Address potential future developments
    - Provide sample pragmatic policies and practices that, if followed, allow any Indiana business to implement the cybersecurity and risk mitigation practices identified by the PII Working Group

- **Additional Notes**
  - All referenced Research Conducted is available via the embedded link or as an attachment to this document.

- **Attachments**
  - State of Indiana Additional Terms and Conditions – SaaS
  - State of Indiana Information Privacy Policy

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. **IU Health:**
        i. Centers for Medicare & Medicaid Services (CMS) has released several guidance documents and programs on cybersecurity.
        ii. The Health Information Management Society (HIMSS) currently offers a comprehensive cybersecurity education program, as does the American Hospital Association (AHA), and American Health Information Management Association (AHIMA). In addition, the National Health Information Sharing and Advisory Center (NH-ISAC) also offers guidance to organizations, as does Infragard. HITRUST, which is a for-profit organization, is also popular with many large health systems and payers. HITRUST provides guidance and a security framework (HITRUST Common Security Framework or CSF).
        iii. However, much of this education is focused on either the basics or is aimed at highly sophisticated organizations, which is not the majority of healthcare.
    b. **Department of Revenue (DOR):**
        i. Provided annual awareness training to all employees, contractors, temps, vendors; facilitated business continuity and incident response exercises; and disseminated notifications about real-world security events, issues and best practices to the entire agency.
    c. **KAR Auction:**
        i. We cannot speak for the area in general; however, most cybersecurity programs are realistically less than 5 years old and have focused on "don't click on the link". The real issue here is critical thinking and how to discern what is being asked. For instance, you probably do not have a rich uncle elsewhere in the world that wants to give you money.
    d. **Citizens Energy:**
        i. We have done a significant amount of this to the BOD, and to Senior management through Risk Management efforts.
    e. **Briljent:**
        i. Very little, small business responds to the market at a rate that aligns with their budgets.
        ii. We have updated our annual user training and continue to push out updates to patch for new vulnerabilities.
    f. **RCR Technology:**
        i. We have developed multiple education PowerPoints that outline the key security issues and provided training to key developer areas.
        ii. Security resources continue to attend local and nearby security conferences whenever possible.
        iii. Completed all of the Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (Mars-e) version 2 security requirements which are **very** extensive.
        iv. We continue to assess and enhance all areas of security maturing our security stance over time.

v. We perform external penetration testing and run numerous other tools to assess the vulnerability of our systems from inside and outside the network.
vi. We perform our own personal assessments of cybersecurity that are based on industry knowledge and expertise as well as a variety of industry known methodologies.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. **IU Health:**
        i. Currently we believe those to be the continuing maintenance and upgrading of systems to protect against new and emerging threats, the abundance of legacy systems, the continuing issues with workflows, the lack of consistent training and education, and the economic pressures causing a de-emphasis on cyber due to having to keep the lights on in many organizations.
    b. **DOR:**
        i. External threats, malicious insiders, employees who fall for social engineering schemes, and sensitive data outside of the State's protected zone.
    c. **KAR Auction:**
        i. Unknowledgeable staff and weak technical controls for user-based activity. For example, protecting from inbound emails, web filtering, etc.
    d. **Citizens Energy:**
        i. We typically store a significant amount of PII to include social security numbers (SSN), banking information, and medical records.
    e. **Briljent:**
        i. As a small business, we are a hub of information for our employees and their families. Banking, medical, PII, passwords, network activity, etc. are all vulnerabilities that need to be considered.
    f. **RCR Technology:**
        i. The largest vulnerabilities are ones that are owned by the Indiana Office of Technology (IOT)
        ii. We are not able to update without their concurrence and support, and in some cases funding. This is not blaming them, only that they own and manage a lot of the essential infrastructure.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. **IU Health:**
        i. The need to provide basic education that is relevant to organizations to show them how to protect, as opposed to the constant emphasis on data breaches.
    b. **DOR:**
        i. Funding and manpower to support security assessments and implementation of security enhancements.
    c. **KAR Auction:**
        i. Encryption or pseudo anonymization

d. **Citizens Energy:**
    i. We believe medical records. HIPPA does not have any fines for violations. They leave this to the States. Indiana does not have any strong regulation to ensure compliance with HIPPA. In addition, Indiana Health Information Exchange (IHIE) is not regulated, and does not allow owners of the data in their database opt out. When one is able to opt out of the IHIE database, the data is not entirely removed; rather, it is only restricted from select searches and/or usage.
e. **Briljent:**
    i. Being secure with minimal budget and expertise
    ii. Intrusion detection
f. **RCR Technology:**
    i. Funding for security resources and expertise building through external training boot camps and conferences
    ii. Lack of a consolidated security information and event management tool that collects and combines all potential security events along with correlating all security data in one tool throughout the State's network.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. **IU Health:**
        i. We are required to follow the HIPAA Privacy and Security Rules, HITECH Act, Stark Act, and a number of state and local laws.
    b. **DOR:**
        i. Internal Revenue Service (IRS) publication 1075, National Institute of Standards and Technology (NIST) special publication 800-53 and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), State code, and state agency policy and standards.
    c. **KAR Auction:**
        i. HIPAA, Telephone Consumer Protection Act (TCPA), COPPA, General Data Protection Regulation (GDPR), Personal Information Protection and Electronic Documents Act (PIPEDA), Freedom of Information and Protection of Privacy Act (FIPPA), etc.
    d. **Citizens Energy:**
        i. Strong state laws on PII. The definition of PII is somewhat vague and does not stay current with data being kept by businesses.

    e. **Briljent:**
        i. We have audits of our systems by the Centers for Medicare and Medicaid Services to ensure compliance because we are a federal contractor. That is rare for a business our size outside of the niche of government contractors.
        ii. Not all of our work is affected by it, but we are primarily concerned about HIPAA due to the nature of our client work.
    f. **RCR Technology:**
        i. CMS Mars-e v2 requirements

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. **IU Health:**
        i. We have highlighted the NH-ISAC Threat Intelligence Committees (TIC) and Cyberfit programs as great examples for how multiple organizations can work together to identify, classify, and mitigate threats across a large population.
        ii. We have also discussed how organizations are already self-organizing, specifically with Jennings Aske's work at Columbia/NYP.
    b. **DOR:**
        i. The Information Security Research and Education (INSuRE) program researches and seeks solutions to hard security problems. INSuRE members are the US Intelligence Community, US National Laboratories, US universities and colleges that include Purdue, and State government organizations that include IOT.
    c. **KAR Auction:**
        i. We would look at GDPR as an indication of where privacy or safeguarding sensitive information is going.
    d. **RCR Technology:**
        i. NIST Cybersecurity framework, https://www.nist.gov/cyberframework
        ii. Center for Internet Security (CIS) Critical Security Controls, https://www.cisecurity.org/controls/
        iii. SANS Institute top 20 critical security controls, https://www.sans.org/security-resources/posters/20-critical-security-controls/55/download

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. **DOR:**
        i. DOR white paper defining sensitive data that DOR must protect
        ii. DOR Protection of Taxpayer Information Job Aid
        iii. Department of Homeland Security (DHS) Factsheet on Safeguarding PII
        iv. DHS Handbook for Safeguarding Sensitive PII
    b. **RCR Technology:**
        i. Most of what is available is good, but not useful in validating true expertise and experience.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. **IU Health:**
        i. They are currently utilizing the same sources we are, plus also self-organizing as part of emergency management to address these issues.
    b. **DOR:**
        i. The IRS requires anyone receiving Federal Tax Information (FTI) to receive security awareness training, additional security training for specific roles, and contingency and incident response training for pertinent personnel.

c. **Briljent:**
    i. As many others do, we comply with contract regulations and hope that suits the rest of our business functions well.
d. **RCR Technology:**
    i. They are provided with sizable budgets for security conferences, training and boot camps. This is essential.

8. What does success look like for your area in one year, three years, and five years?

a. **IU Health:**
    i. Year 1:
        1. Begin developing a pilot program modeled after NH-ISAC's TICs to collaborate across multiple institutions to address security issues and provide a means for healthcare organizations to contact us to report potential issues. Beginnings of a communication plan designed to reach out to healthcare providers.
    ii. Year 3:
        1. Expansion of the program to have more dedicated staff and interaction with providers. More proactive education, collaboration with other states, and organizations such as NH-ISAC, Infragard, and DHS to provide cybersecurity awareness.
    iii. Year 5:
        1. Having this program as part of normal business of the State.
b. **DOR:**
    i. Year 1: Implement the performance of annual security assessments and security controls for severe and significant findings.
    ii. Year 3 & 5: Help vendors, partners, and tax e-filing community become compliant with DOR security; improve agency access controls, data security, and vulnerability management; and normalize annual business continuity/disaster recovery planning and testing.
c. **Briljent:**
    i. Compliance with state and federal programs in coalition with comparable businesses to share cost and expertise
    ii. Preventing a cybersecurity incident outright, or preventing a cybersecurity incident from having a business impact.
d. **RCR Technology:**
    i. This is very difficult to quantify, but success is measured by at least two key metrics:
    ii. Security assessment performed against the network and key resources. The assessment should show that all High and most Medium level risks are mitigated and/or actions are in place to compensate and/or address these risks. Compensating and/or addressing the risks should happen within a reasonable timeframe, to a degree that is understood, and approved by the State. Key factors the security assessment would need to include are the industry known security threats that exist.
    iii. All compliance requirements in the area of cybersecurity are achieved, and/or plans of action are approved

9. **What are the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. **IU Health:**
        i. There needs to be a concerted effort to reach out to specific medical providers to specifically address what they need to do to increase security. People are very aware of the need for cybersecurity. The specific guidance that they need to be secure has been either too specific or lacking.
    b. **DOR:**
        i. The public should be apprised that DOR continuously implements tools and processes to bolster cybersecurity to protect their information, which may appear inconvenient to them. For example, we may require taxpayers logging into our applications to increase the length and complexity of their passwords.
    c. **KAR Auction:**
        i. Realistically, the biggest area is to help people understand how to protect themselves. Does that phone application you are installing really need geo-location tracking services, do you really need to give up your contacts? How to turn off base services on your Android or iOS.
    d. **Briljent:**
        i. We believe there is a serious need for public outreach and education around cybersecurity so that risk can be further understood and personal decisions made with that risk in mind.
        ii. More online training provided by the State would help.
    e. **RCR Technology:**
        i. Provide the funding for at least 2 major security conferences and 2 security training classes per year.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. **IU Health:**
        i. According to the 2015 Bureau of Labor Statistics (BLS), 9.0% of the total workforce in Indiana is in healthcare.
        ii. There are no clear statistics as to how much of that section workforce is cybersecurity related.
        iii. IU Health employs approximately 30,000 people. Approximately 550 personnel work in information technology (IT), which is approximately 2% of the workforce. Of that, 20 staff members are dedicated to cybersecurity full-time. Which is approximately 0.07% of the total workforce.
        iv. According to a Frost & Sullivan report, 30% of healthcare hiring managers plan to increase staff by 20% or more, and 9% want to hire between 16% and 20% additional personnel.

v. However, because of a lack of risk assessments and actual planning, according to the May 2017 Health Care Industry Cybersecurity Task Force task report, this number is not even close to accurate. Further analysis of BLS 2016-2026 statistics, in combination with the sources indicating that we need hundreds of thousands of jobs to fill cybersecurity vacancies, indicate that the number is closer to 50,000 in the US.

vi. The issue is not cybersecurity jobs, it is getting people to understand cybersecurity and exercise due diligence.

b. **DOR:**

i. Total DOR Workforce as of December 2017: 751. We have 659 FTEs and 92 contractors.

ii. Total DOR Cybersecurity Staff: 6

iii. Total DOR Cybersecurity Staff shortfall: 0

c. **KAR Auction:**

i. We cannot answer for this area, but the cybersecurity footprint of any company is remarkably small. Average companies that have security departments are relatively small in comparison to large corporations (e.g. Target, Home Depot, and Equifax). Because many businesses have little understanding of cybersecurity, this may account for the small to non-existent dedicated security personnel employed in smaller Indianapolis businesses.

d. **RCR Technology:**

i. Workforce: 120 people

ii. Cybersecurity: 1.5 people

iii. We need 2 people

11. What do we need to do to attract cyber companies to Indiana?

a. **IU Health:**

i. Advertise and leverage the educational advantage that Indiana has with IU, Purdue, IUPUI, Rose-Hulman, and Notre Dame. Two of the best and most well-connected cyber programs in the country are here, and there are already a number of tech companies, specifically Salesforce, taking full advantage of that. Facilitating business development and encouraging companies to locate offices and/or staff here based on the availability of top-level graduates, quality of living, and low cost would greatly assist.

b. **KAR Auction:**

i. Build the community. Security people are insular and do not talk. We need them to be comfortable to share information, mentor and lead. Additionally, we need to pull in some security-based companies. The smaller local boutique firms are great, but it is not a state focus as it is not well understood.

c. **Citizens Energy:**

i. Grow the corporate headquarters in Indiana. This creates the need for cybersecurity companies.

d. **Briljent:**

i. Show that Indiana has strong growth in the technology sector.

12. What are your communication protocols in a cyber emergency?

a. **IU Health:**
   i. We follow the Hospital Incident Command System (HICS) to escalate incidents. We now have coordinated communication with multiple agencies and will follow the same protocols as a standard multi-site incident. Ultimately, a multidisciplinary approach in healthcare is needed that utilizes HICS as patient safety has to be paramount.

b. **DOR:**
   i. We communicate based on our formalized process of identifying, analyzing, responding to, and recovering from incidents to include cyber emergencies.

c. **KAR Auction:**
   i. Electronic, cell-based

d. **Briljent:**
   i. Email is the preferred method of communication. We generally notify all users, even those that may not be directly affected by a cybersecurity threat.

e. **RCR Technology:**
   i. The State has a planned outlined.

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. **IU Health:**
   i. Focus on assessing risk, and helping people understand what to do to address it. The issue is that we do not focus on the fundamentals, and need to treat cybersecurity as part of the business rather than something to address separately. The more we focus on it as a separate discipline, the less we will be able to attack root causes of many of these issues.

b. **DOR:**
   i. Defense in-depth: an information assurance concept in which multiple layers of security controls are placed throughout an information technology system
   ii. Initial and annual security awareness training
   iii. Phishing testing

c. **Briljent:**
   i. Much of the federal guidance is applicable at the state level as well.

Deliverable: Indiana PII Guidebook

Deliverable: Indiana PII Guidebook

General Information

1. **What is the deliverable?**
    a. The Indiana PII Guidebook will consist of the following:
        i. Define PII
        ii. Characterize the current state
        iii. Identify related regulations
        iv. Identify best practices across all sectors
        v. Address potential future developments
        vi. Provide sample pragmatic policies and practices that, if followed, allow any Indiana business to implement the cybersecurity and risk mitigation practices identified by the PII Working Group

2. **What is the status of this deliverable?**
    a. In-progress; 25% complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Enhanced knowledge of what we should be protecting.
    b. This provides an actionable blueprint to Hoosier businesses to protect the privacy of individually-identifiable information.
    c. Provide quick-reference visibility into best practices.
    d. Ensuring a well-rounded output by the PII Working Group.
    e. Providing context around potential result of technological advancement, today's policy decisions, etc.
    f. Recognition of current posture is important to understand where we need to be.

6. **What metric or measurement will be used to define success?**
    a. All-encompassing definition and ease of application by end users.
    b. Generation of an all-encompassing reference list for PII Working Group use.
    c. Robust assessment of the current state.
    d. Usability by a broad swath of Hoosier businesses.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. All those who are working to define PII and those who would like context behind PII.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Unknown

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Sector-specific groups or all sectors will be engaged on an as-needed basis.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Any on an as-needed basis.

12. **Who should be main lead of this deliverable?**
    a. PII Working Group

13. What are the expected challenges to completing this deliverable?

a. Ensuring that definition has high utility to various sectors.
b. Providing an end-product that is sufficiently all encompassing so as to be valuable for a large number of users.
c. Accurately capturing all PII best practices.
d. Difficult to capture all regulations across all sectors.
e. Difficult to tell the future in any space, especially technology.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Define PII	Richard Braidich & Tony Chu	25%	End of Q4, 2018	
Characterize the current state	Ashley Schenck	25%	End of Q4, 2018	
Identify related regulations	Ted Cotterill	25%	End of Q4, 2018	
Identify best practices across all sectors	Valita Fredland	25%	End of Q4, 2018	
Address potential future developments	Leon Ravenna & Mitch Parker	25%	End of Q4, 2018	
Provide sample pragmatic policies and practices that, if followed, allow any Indiana business to implement the cybersecurity and risk mitigation practices identified by the PII Working Group	Dom Caristi	25%	End of Q4, 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No
b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. A cross-sector body of subject-matter experts is required to form an understanding of Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment. To provide Hoosiers with a foundational understanding of that which we intend to protect, the Personally Identifiable Information Working Group will create the Indiana PII Guidebook. This is intended to do the following:
   i. define PII
   ii. characterize the current state
   iii. identify related regulations
   iv. identify best practices across all sectors
   v. address potential future developments; and
   vi. provide sample pragmatic policies and practices that, if followed, allow any Indiana business to implement the cybersecurity and risk mitigation practices identified by the PII Working Group.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This deliverable compliments the work of other components of the Indiana Executive Council on Cybersecurity by providing both a foundational understanding of personally identifiable information as well as articulating how the definition can be applied to specific information maintained by any number of Hoosier businesses.
b. Costs associated with the enhanced knowledge regarding PII are unknown.

19. What is the risk or cost of not completing this deliverable?

a. This deliverable will be completed by the PII Working Group. If it were not completed, Hoosiers would not realize the benefit of added knowledge about the core data elements that must be protected.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. A completed and approved Indiana PII Guidebook defines the success of this deliverable.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Unknown. At this time, PII Working Group members remain engaged and related tactics are well defined. Ownership of each has been assigned.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. N/A

b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. The PII Working Group is striving to provide a Guidebook that provides a definition of PII that can be leveraged by all business sectors across Indiana. As such, the definition is unlikely to be limited to fixed data elements that are commonly thought of as direct identifiers. It is more likely that the definition will provide a framework or PII-related decision tree that can be applied to any business situation.

b. The avoidance of a fixed-element definition will lend itself to a more lasting benefit for Hoosiers. However, periodic review and revision by subject matter experts may be required to ensure that the Indiana PII Guidebook remains relevant.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. The PII Working Group is made up of members that maintain a depth and breadth of knowledge in the realm that is unparalleled across the State of Indiana. Members have consulted bodies of knowledge on the subject and intend to communicate that knowledge in a consumable way that enables real action by Hoosiers.

27. Can this deliverable be used by other sectors?

a. Yes.

b. **If Yes, please list sectors**

i. All.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes.

30. What are other public relations and/or marketing considerations to be noted?

a. IECC lead-agency communications directors should be made aware of the Indiana PII Guidebook and align with an appropriate marketing strategy.

Evaluation Methodology

Objective 1: IECC PII Working Group develop an Indiana PII Guidebook for government and general public by the end of Q1, 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Department of Revenue PII Research Responses
- State of Indiana Additional Terms and Conditions – Software as a Service (SaaS)
- State of Indiana Information Privacy Policy

Department of Revenue (DOR)

PII Research Responses

2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

COMMITTEE AND WORKING GROUP QUESTIONNAIRE – RESEARCH PHASE

Instructions: As your committee or working group is in the Research Phase, it is important we work with other committees and working groups to get the information your team will need to be successful. Please answer the questions the best you can.

Provide your questions and answers to MosleyCLM@iot.in.gov no later than ***Jan. 10, 2018.***

Committee/Working Group: Personally Identifiable Information Working Group

Person Submitting Summary: Tony Chu

Email of Person Submitting: TChu@dor.in.gov

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. **Department of Revenue (DOR):**
        i. Provided security awareness training to all full time employees (FTE), contractors, temps, and vendors at on-boarding and annually thereafter. This training apprises employees of the data they must protect, and the methods by which they must be protected.
        ii. Led a Continuity of Operations plan exercise in 2014 and the next one is projected for 2018.
        iii. Trained and exercised the DOR Incident Response team and plan annually.
        iv. Sent periodic e-mails and published articles in agency publications apprising DOR-all of security issues and best security practices.
        v. Sent e-mails to DOR-all apprising them of urgent real-world security issues, and how to address them (e.g., phishing messages and phone-based social engineering attacks)

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. **DOR:**
        i. External threats: State and non-state cyber actors, cybercriminals, cyberterrorists, etc.
        ii. Malicious insiders
        iii. Employees who fall for social engineering schemes
        iv. Servers containing sensitive data that reside outside of the state's protected zone (PZ)

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. **DOR:**
        i. Internal Revenue Service (IRS) Publication 1075
        ii. National Institute of Standards and Technology (NIST) Special Publication 800-53: Using Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) for detailed security assessments
        iii. Indiana Code and policies
        iv. IOT policies and standards
        v. DOR policies and procedures

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. **DOR:**
        i. All other state departments of revenue/taxation that receive Federal Tax Information (FTI) are required by IRS to provide:
            1. Security awareness training to all employees
            2. Role-based training to personnel based on assigned security roles and responsibilities
            3. Contingency training to personnel responsible for recovering backup copies of FTI
            4. Incident response training to personnel responsible for handling and reporting security events

8. **What does success look like for your area in one year, three years, and five years?**
    a. **DOR:**
        i. Year 1:
            1. Conduct security assessments
            2. Implement security controls address severe and significant vulnerabilities and threats
        ii. Year 3:
            1. DOR, its vendors, partners, and e-filing tax community comply with DOR security requirements
            2. Work towards the following goals
                a. All sensitive DOR servers reside in the state's PZ
                b. DOR servers reside in appropriate network segments

c. All sensitive DOR data within the state network is encrypted at rest and in motion
d. DOR users have least privileged access
e. Security patching is done immediately
f. Continuity of Operations (COOP) and Disaster Recovery (DR) plans are developed, appropriately resourced, and successfully tested

iii. Year 5:
1. Achieve the following goals
a. All sensitive DOR servers reside in the state's PZ
b. DOR servers reside in appropriate network segments
c. All sensitive DOR data within the state network is encrypted at rest and in motion
d. DOR users have least privileged access
e. Security patching is done immediately
f. COOP and DR plans are developed, appropriately resourced, and successfully tested

12. What are your communication protocols in a cyber emergency?

a. **DOR:**
i. DOR employee, Indiana Office of Technology (IOT) employee, or anyone else identifies and reports suspicious activities to DOR Security Team.
ii. DOR security team assesses and analyzes the situation to determine if there is an emergency.
iii. DOR security team, upon DOR chief information officer (CIO) approval, takes immediate action as necessary to stop the perpetuation of damage.
iv. DOR security team develops multiple courses of action (COA) to address remaining security concerns and to recover from the event. They then present the COAs to other members of the DOR incident response team comprising of DOR chief operating officer, DOR chief information officer, DOR inspector general, DOR legal team, DOR communications team, and IOT chief information security officer.
v. DOR incident response team decides on a single course of action.
vi. DOR incident response team briefs DOR commissioner on the situation, actions taken, and proposed COA.
vii. DOR commissioner approves COA
viii. DOR incident response team works with IOT to execute the approved COA.

State of Indiana Additional Terms and Conditions

Software as a Service (SaaS)

March 2017

State of Indiana Additional Terms and Conditions
Software as a Service Engagements

Exhibit 1 to the Contract between the State acting through [agency name] and the Contractor.

DEFINITIONS

Data means all information, whether in oral, written, or electronic form, created by or in any way originating with the State, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or that in any way originated with the State, in the course of using and configuring the Services.

Data Breach means any actual or reasonably suspected unauthorized access to or acquisition of Encrypted Data.

Encrypted Data means Data that that is required to be encrypted under the contract and Statement of Work.

Indiana Office of Technology means the agency established by Ind. Code § 4-13.1-2-1.

Information Security Framework means the State of Indiana's written policy and standards document governing matters affecting security and available at http://www.in.gov/iot/2339.htm.

Security Incident means any actual or reasonably suspected unauthorized access to the contractor's system, regardless of whether contractor is aware of a Data Breach. A Security Incident may or may not become a Data Breach.

Service(s) means that which is provided to the State by contractor pursuant to this contract and the contractors obligations under the contract.

Service Level Agreement means a written agreement between both the State and the contractor that is subject to the terms and conditions of this contract. Service Level Agreements should include: (1) the technical service level performance promises (i.e. metrics for performance and intervals for measure); (2) description of service quality; (3) identification of roles and responsibilities; (4) remedies, such as credits; and (5) an explanation of how remedies or credits are calculated and issued.

Statement of Work means the written agreement between both the State and contractor attached to and incorporated into this contract.

TERMS

1. Data Ownership: The State owns all rights, title, and interest in the Data. The contractor shall not access State user accounts or Data, except: (1) in the normal course of data center operations; (2) in response to Service or technical issues; (3) as required by the express terms of this contract, applicable Statement of Work, or applicable Service Level Agreement; or (4) at the State's written request.

Contractor shall not collect, access, or use Data except as strictly necessary to provide Service to the State. No information regarding State's use of the Service may be disclosed, provided, rented, or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this contract.

2. Data Protection: Protection of personal privacy and Data shall be an integral part of the business activities of the contractor to ensure there is no inappropriate or unauthorized use of Data at any time. To this end, the contractor shall safeguard the confidentiality, integrity, and availability of Data and shall comply with the following conditions:

a. The contractor shall implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, or theft of Data. Contractor shall implement and maintain heightened security measures with respect to Encrypted Data. Such security measures shall be in accordance with Indiana Office of Technology practice and recognized industry practice, including but not limited to the following:

1. Information Security Framework; and

2. Indiana Office of Technology Cloud Product and Service Agreements, Standard ID: IOT-CS-SEC-010.

b. All Encrypted Data shall be subject to controlled access. Any stipulation of responsibilities shall be included in the Statement of Work and will identify specific roles and responsibilities.

c. The contractor shall encrypt all Data at rest and in transit. The State may, in the Statement of Work, identify Data it deems as that which may be publicly disclosed that is not subject to encryption. Data so designated may be maintained without encryption at rest and in transit. The level of protection and encryption for all Encrypted Data shall meet or exceed that required in the Information Security Framework.

d. At no time shall any Data or processes — that either belong to or are intended for the use of State — be copied, disclosed, or retained by the contractor or any party related to the contractor for subsequent use in any transaction that does not include the State.

e. The contractor shall not use any information collected in connection with the Services for any purpose other than fulfilling its obligations under the contract.

3. Data Location: Storage of Data at rest shall be located solely in data centers in the United States and the contractor shall provide its Services to the State and its end users solely from locations in the United States. The contractor shall not store Data on portable devices, including personal laptop and desktop computers. The contractor shall access Data remotely only as required to provide technical support. The

contractor shall provide technical user support on a 24/7 basis unless specified otherwise in the Service Level Agreement.

4. Notice Regarding Security Incident or Data Breach:

a. Incident Response: contractor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries, and seeking external expertise as mutually agreed upon, defined by law, or contained in the contract. Discussing Security Incidents and Data Breaches with the State must be handled on an urgent basis, as part of contractor's communication and mitigation processes as mutually agreed upon in the Service Level Agreement, contained in the contract, and in accordance with IC 4-1-11 and IC 24-4.9 as they may apply.

b. Security Incident Reporting Requirements: The contractor shall report a Security Incident to the State-identified contact(s) as soon as possible by telephone and email, but in no case later than two (2) days after the Security Incident occurs. Notice requirements may be clarified in the Service Level Agreement and shall be construed in accordance with IC 4-1-11 and IC 24-4.9 as they may apply.

c. Data Breach Reporting Requirements: If a Data Breach occurs, the contractor shall do the following in accordance with IC 4-1-11 and IC 24-4.9 as they may apply: (1) as soon as possible notify the State-identified contact(s) by telephone and email, but in no case later than two (2) days after the Data Breach occurs unless a shorter notice period is required by applicable law; and (2) take commercially-reasonable measures to address the Data Breach in a timely manner. Notice requirements may be clarified in the Service Level Agreement. If the Data involved in the Data Breach involves protected health information, personally identifying information, social security numbers, or otherwise confidential information, other sections of this contract may apply. The requirements discussed in those sections must be met in addition to the requirements of this section.

5. Responsibilities Regarding Data Breach: This section applies when a Data Breach occurs with respect to Encrypted Data within the possession or control of the contractor.

a. The contractor shall: (1) cooperate with the State as reasonably requested by the State to investigate and resolve the Data Breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document and provide to the State responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the Services, if necessary.

b. Unless stipulated otherwise in the Statement of Work, if a Data Breach is a result of the contractor's breach of its contractual obligation to encrypt Data or otherwise prevent its release as reasonably determined by the State, the contractor shall bear the costs associated with: (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators, or others required by federal and/or state law, or as otherwise agreed to in the Statement of Work; (3) a credit monitoring service required by federal and/or state law, or as otherwise agreed to in the Statement of Work; (4) a website or a toll-free number and call center for affected individuals required by federal and/or state law — all of which shall not amount to less than the average per-record per-person cost calculated for data breaches in the United States (in, for example, the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach); and (5) complete all

corrective actions as reasonably determined by contractor based on root cause and on advice received from the Indiana Office of Technology. If the Data involved in the Data Breach involves protected health information, personally identifying information, social security numbers, or otherwise confidential information, other sections of this contract may apply. The requirements discussed in those sections must be met in addition to the requirements of this section.

6. Notification of Legal Requests: If the contractor is requested or required by deposition or written questions, interrogatories, requests for production of documents, subpoena, investigative demand or similar process to disclose any Data, the contractor will provide prompt written notice to the State and will cooperate with the State's efforts to obtain an appropriate protective order or other reasonable assurance that such Data will be accorded confidential treatment that the State may deem necessary.

7. Termination and Suspension of Service:

a. In the event of a termination of the contract, the contractor shall implement an orderly return of Data in a mutually agreeable and readable format. The contractor shall provide to the State any information that may be required to determine relationships between data rows or columns. It shall do so at a time agreed to by the parties or shall allow the State to extract its Data. Upon confirmation from the State, the contractor shall securely dispose of the Data.

b. During any period of Service suspension, the contractor shall not take any action that results in the erasure of Data or otherwise dispose of any of the Data.

c. In the event of termination of any Services or contract in its entirety, the contractor shall not take any action that results in the erasure of Data until such time as the State provides notice to contractor of confirmation of successful transmission of all Data to the State or to the State's chosen vendor.

During this period, the contractor shall make reasonable efforts to facilitate the successful transmission of Data. The contractor shall be reimbursed for all phase-out costs (i.e., costs incurred within the agreed period after contract expiration or termination that result from the transfer of Data or other information to the State). A reimbursement rate shall be agreed upon by the parties during contract negotiation and shall be memorialized in the Statement of Work. After such period, the contractor shall have no obligation to maintain or provide any Data and shall thereafter, unless legally prohibited, delete all Data in its systems or otherwise in its possession or under its control. The State shall be entitled to any post-termination assistance generally made available with respect to the Services, unless a unique data retrieval arrangement has been established as part of a Service Level Agreement.

d. Upon termination of the Services or the contract in its entirety, contractor shall, within 30 days of receipt of the State's notice given in 7(c) above, securely dispose of all Data in all of its forms, including but not limited to, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the State upon completion.

8. Background Checks: The contractor shall conduct a Federal Bureau of Investigation Identity History Summary Check for each employee involved in provision of Services: (1) upon commencement of the contract; (2) prior to hiring a new employee; and (3) for any employee upon the request of the State. The contractor shall not utilize any staff, including subcontractors, to fulfill the obligations of the

contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to one (1) year is an authorized penalty. The contractor shall promote and maintain an awareness of the importance of securing the State's information among the contractor's employees, subcontractors, and agents. If any individual providing Services under the contract is not acceptable to the State, in its sole opinion, as a result of the background or criminal history investigation, the State, in its sole option shall have the right to either: (1) request immediate replacement of the individual; or (2) immediately terminate the contract, related Statement of Work, and related Service Level Agreement.

9. Access to Security Logs and Reports: The contractor shall provide to the State reports on a schedule and in a format specified in the Service Level Agreement as agreed to by both the contractor and the State. Reports shall include latency statistics, user access, user access IP address, user access history, and security logs for all Data. The State's audit requirements shall, if applicable, be defined in the Statement of Work.

10. Contract Audit: The contractor shall allow the State to audit conformance to the contract terms. The State may perform this audit or contract with a third party at its discretion and at the State's expense.

11. Data Center Audit: The contractor shall perform an annual independent audit of its data center(s) where Data, State applications, or other State information is maintained. The contractor shall perform this independent audit at its expense and shall, upon completion, provide an unredacted version of the complete audit report to the State. (The contractor may redact its proprietary information from the unredacted version, however.) A Service Organization Control (SOC) 2 audit report or equivalent approved by the Indiana Office of Technology sets the minimum level of a third-party audit.

The State may perform an annual audit of contractor's data center(s) where Data, State applications, or other State information is maintained. The audit may take place onsite or remotely, at the State's discretion. The State shall provide to contractor thirty (30) days' advance notice prior to the audit. The contractor will make reasonable efforts to facilitate the audit and will make available to the State members of its staff during the audit. The State may contract with a third party to conduct the audit at its discretion and at the State's expense. If the contractor maintains Data, State applications, or other State information at multiple data centers, the State may perform an annual audit of each data center.

The parties agree that any documents provided to the State under this paragraph shall be deemed a trade secret of contractor and is deemed administrative or technical information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under the Indiana Access to Public Records Act, IC 5-14-3.

12. Change Control and Advance Notice: The contractor shall give notice to the State for change management requests. Contractor shall provide notice to the State regarding change management requests that do not constitute an emergency change management request at least two (2) weeks in advance of implementation. Contractor shall provide notice to the State regarding emergency change management requests no more than twenty-four (24) hours after implementation.

Contractor shall make updates and upgrades available to the State at no additional cost when contractor

makes such updates and upgrades generally available to its users. No update, upgrade, or other change to the Service may decrease the Service's functionality, adversely affect State's use of or access to the Service, or increase the cost of the Service to the State.

13. Security: The contractor shall, on an annual basis, disclose its non-proprietary system security plans or security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the contractor. For example: virus checking and port sniffing. The State and the contractor shall share information sufficient to understand each other's roles and responsibilities. The contractor shall take into consideration feedback from the Indiana Office of Technology with respect to the contractor's system security plans.

The parties agree that any documents provided to the State under this paragraph shall be deemed a trade secret of contractor and is deemed administrative or technical information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under the Indiana Access to Public Records Act, IC 5-14-3.

14. Non-disclosure and Separation of Duties: The contractor shall enforce role-based access control, separation of job duties, require commercially-reasonable nondisclosure agreements, and limit staff knowledge of Data to that which is absolutely necessary to perform job duties. The contractor shall annually provide to the State a list of individuals that have access to the Data and/or the ability to service the systems that maintain the Data.

15. Import and Export of Data: The State shall have the ability to import or export Data in piecemeal or in entirety at its discretion, with reasonable assistance provided by the contractor, at any time during the term of contract. This includes the ability for the State to import or export Data to/from other parties at the State's sole discretion. Contractor shall specify in the Statement of Work if the State is required to provide its' own tools for this purpose, including the optional purchase of contractor's tools if contractor's applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The contractor shall be responsible for the acquisition and operation of all hardware, software, and network support related to the Services being provided. The technical and professional activities required for establishing, managing, and maintaining the environments are the responsibilities of the contractor. Subject to the Service Level Agreement, the Services shall be available to the State at all times. The contractor shall allow the State to access and use the Service to perform synthetic transaction performance testing.

The contractor shall investigate and provide to the State a detailed incident report regarding any unplanned Service interruptions or outages. The State may terminate the contract for cause if, at its sole discretion, it determines that the frequency of contractor-preventable outages is sufficient to warrant termination.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to Services, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the contractor, and who may be involved in any application development and/or operations.

The contractor shall be responsible for the acts and omissions of its subcontractors, strategic business partners, or other entities or individuals who provide or are involved in the provision of Services.

18. Business Continuity and Disaster Recovery: The State's recovery time objective shall be defined in the Service Level Agreement. The contractor shall ensure that the State's recovery time objective has been met and tested as detailed in the Service Level Agreement. The contractor shall annually provide to the State a business continuity and disaster recovery plan which details how the State's recovery time objective has been met and tested. The parties agree that any documents provided to the State under this paragraph shall be deemed administrative or technical information that would jeopardize a record keeping or security system, and shall be exempt from disclosure under the Indiana Access to Public Records Act, IC 5-14-3. The contractor shall work with the State to perform an annual disaster recovery test and take action to correct any issues detected during the test in a time frame mutually agreed upon between the contractor and the State in the Service Level Agreement.

The State's Data shall be maintained in accordance with the applicable State records retention requirement, as determined by the State. The contractor shall annually provide to the State a resource utilization assessment detailing the Data maintained by the contractor. This report shall include the volume of Data, the file formats, and other content classifications as determined by the State.

19. Compliance with Accessibility Standards: The contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the State.

20. State Additional Terms and Conditions Revision Declaration: The clauses in this Exhibit have not been altered, modified, changed, or deleted in any way except for the following clauses which are named below:_____

State of Indiana
Information Privacy Policy

September 2017

State of Indiana Information Privacy Policy

Version: 1 (9/15/17)

Contents

Purpose 2

Applicability 2

Authority 2

Definitions 2

Background 2

Policy 2

- Leadership & Accountability 3
- Privacy Risk Management and Compliance Documentation 4
- Information Security 5
- Incident Response 5
- Notice and Redress for Individuals 6
- Privacy Awareness 7

References 8

Revision History 8

Approval 8

Purpose

The purpose of this Policy is to ensure that data maintained by the State of Indiana is kept and treated in accordance with applicable laws and regulations. This policy will provide guidance to State agencies as they work to maintain the privacy of those they serve.

Applicability

This Policy shall apply to all Government Information. Nothing contained in this Policy shall be construed to require an agency to expend funds for the sole purpose of obtaining compliance with this Policy. However, at such time as information technology systems are procured or altered, an agency shall consult with the MPH and shall make reasonable efforts to obtain compliance with this Policy.

Authority

This Policy is promulgated by the Indiana Management Performance Hub pursuant to IC 4-3-26-10(3).

Definitions

1. "APO" means an Agency Privacy Officer as discussed herein.
2. "CPO" means the Chief Privacy Officer of the state.
3. "Government information" has the meaning set forth in IC 4-3-26-7.
4. "IOT" means the Indiana Office of Technology established by IC 4-13.1-2-1.
5. "MPH" means the Indiana Management Performance Hub established by IC 4-3-26-8.
6. "Personal information" has the meaning set forth in IC 4-1-6-1(b).
7. "Policy" means this *State of Indiana Information Privacy Policy*.

Background

Through the daily operations of its agencies, the State of Indiana creates, maintains, and safeguards vast amounts of information relating to its citizens and the governing process. This data is a valuable asset in providing government services to the public as well as informing the policymaking process to ensure the best outcomes for the Hoosiers we serve. Ensuring that Government Information is maintained appropriately is of critical concern.

Policy

Maintaining the privacy of Government Information is ultimately the responsibility of all State agency employees as they create, capture, and store information in the course of their duties. To effectively maintain the privacy of Government Information, State agency employees must understand the content of the Government Information at issue and how that content affects the agency's privacy responsibilities.

The MPH seeks to establish a policy which recognizes and accounts for the relationship and linkage between privacy and security controls, enabling State agencies to more efficiently maintain the privacy of Personal Information. To do so, the MPH puts forth this Policy, which is adapted from *Best Practices: Elements of a Federal Privacy Program*, authored by the Federal CIO Council.[1]

The Policy includes six components, which are essential elements of an effective privacy management program. Those are leadership and accountability, privacy risk management and compliance documentation, information security, incident response, notice and redress for individuals, and privacy awareness.

Each is discussed in greater detail below.

Leadership & Accountability

The State of Indiana's success in the maintenance of individual privacy begins with leadership. IT systems can be built to accommodate varying levels of access, but it is top-down direction that will ensure diligence on the part of State employees. It is on those lines that the MPH recommends the appointment of an Agency Privacy Officer in each agency. As a part-time role, it is suggested that the APO be an individual serving as agency general counsel or records/compliance counsel, creating alignment with the day-to-day duties and the role of APO. The APO will work with the MPH and will be responsible for:

- Ensuring agency compliance with applicable State and Federal laws and regulations;
- Overseeing and coordinating agency privacy compliance efforts;
- Remaining abreast of legislative change regarding privacy in the agency's sphere of operation; and
- Collaborating with other APO's and the Chief Privacy Officer.

Housed in MPH, the CPO can serve as a liaison for intergovernmental, multi-agency, and public-private efforts that involve the privacy of Government Information.

The APO should have a foundational understanding of the Fair Information Practices Act at Ind. Code Ch. 4-1-6, the Access to Public Records Act at Ind. Code Ch. 5-14-3, and any statutes and rules that govern the Government Information at issue with more specificity. The CPO can assist APOs in the review and application of these statutes.

[1] *Best Practices: Elements of a Federal Privacy Program*, Federal CIO Council, (June, 2010), https://energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf.

Privacy Risk Management and Compliance Documentation

As a multifaceted operation, the State of Indiana requires a heightened level of awareness from its subject-matter experts to ensure that Government Information is maintained in a way that respects the privacy of individuals. The APO should have an understanding of current and forthcoming agency efforts that may involve the maintenance, management, or exchange of Government Information. The APO will ensure the inclusion of privacy principles and compliance where appropriate. In certain instances, a privacy impact assessment may be necessary. Such an assessment shall be completed in accordance with applicable IOT standards.[2]

The APO will oversee the annual submission of an information system report as required by Ind. Code. § 4-1-6-7. The information system report will be submitted using the mechanism prescribed by the IOT. The information system report will, at a minimum, include the following:

1) The name or descriptive title of the information system and its location.
2) The nature and purpose of the information system and the statutory or administrative authority for its establishment.
3) The categories of individuals on whom Personal Information is maintained, including the approximate number of all individuals on whom information is maintained and the categories of personal information generally maintained in the system, including identification of those which are stored in computer accessible records and those which are maintained manually.
4) All confidentiality requirements, specifically:
    (A) those information systems or parts thereof which are maintained on a confidential basis pursuant to a statute, contractual obligation, or rule; and
    (B) those information systems maintained on an unrestricted basis.
5) In the case of item (4)(A) above, the agency shall include detailed justification of the need for statutory or regulatory authority to maintain such information systems or parts thereof on a confidential basis.
6) The categories of sources of such Personal Information.
7) The agency's policies and practices regarding the implementation of Ind. Code § 4-1-6-2 relating to information storage, duration of retention of information, and elimination of information from the information system.
8) The uses made by the agency of Personal Information contained in the system.
9) The identity of agency personnel, other agencies, and persons or categories of persons to whom disclosures of personal information are made or to whom access to the system may be granted, together with the purposes therefor and the restriction, if any, on such disclosures and access, including any restrictions on redisclosure.
10) A listing identifying all forms used in the collection of personal information.
11) The name, title, business address, and telephone number of the person immediately responsible for bringing and keeping the system in compliance with the provisions of this chapter.

[2] Data Categorization (IOT-CS-SEC-105); Security Assessment and Authorization (IOT-CS-SEC-146); Collection and Storage of Personal Information (IOT-CS-SEC-103).

Information Security

Pursuant to Ind. Code Art. 4-13.1, the IOT has put forth the State of Indiana Information Security Framework, which provides requirements and direction to inform agency efforts relating to information security.[3] Pursuant to Ind. Code Ch. 5-15-5.1, the Indiana Archives and Records Administration ("ARA") has put forth records retention schedules, which govern the retention and disposition of governmental records.[4] Agencies are expected to be in compliance with both the IOT's Information Security Framework and the ARA's records retention schedules, as they may apply. In context of this Policy and in accordance with Ind. Code § 4-1-6-2, agencies must do the following:

1) Collect, maintain, and use only that Personal Information as is relevant and necessary to accomplish a statutory purpose of the agency.
2) Insofar as possible, segregate information of a confidential nature from that which is a disclosable public record and, pursuant to statutory authority, establish confidentiality requirements and appropriate access controls for all categories of Personal Information contained in the information system.
3) Maintain a list of all persons or organizations having regular access to Personal Information which is not a matter of disclosable public record in the information system.
4) Maintain a complete and accurate record of every access to Personal Information in a system which is not a matter of disclosable public record by any person or organization not having regular access authority.

Incident Response

State agencies are expected to comply with Ind. Code Ch. 4-1-11 and related policies put forth by the IOT. As applicable to state agencies, a breach is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state or local agency. The term does not include the following:

1) Good faith acquisition of personal information by an agency or employee of the agency for purposes of the agency, if the personal information is not used or subject to further unauthorized disclosure.
2) Unauthorized acquisition of a portable electronic device on which personal information is stored if access to the device is protected by a password that has not been disclosed.

Ind. Code § 4-1-11-2.

If such an event occurs, the IOT maintains the Indiana Security Incident Response Team ("ISIRT"), which must be immediately alerted via isirt@iot.IN.gov. The ISIRT will respond and require state agency action in accordance with Information Security Framework Standards *IOT-CS-SEC-133* and *IOT-CS-SEC-134*.

Following the notification and any necessary remediation, the agency must provide to the CPO and ISIRT documentation of the mitigation, disclosure, and notification actions taken.

[3] https://secure.iot.in.gov/.
[4] http://www.in.gov/iara/2360.htm.

Notice and Redress for Individuals

A well-rounded privacy policy should provide for multiple independent verifications that the privacy of individuals is being maintained appropriately. It is on those lines that this Policy restates and reinforces that which the Indiana General Assembly has already put forth. Where a state agency maintains a system and holds title to the Government Information in the system, the agency must provide a mechanism for an individual to challenge, correct, or explain information in a system about the individual. Should a correction or explanation about the Government Information be added to the originating agency's system, that agency must notify other state agencies maintaining copies of the Government Information to ensure that all records are updated accordingly.

> Unless otherwise prohibited by law, any state agency that maintains a Personal Information system shall, upon request and proper identification of any data subject, or a data subject's authorized agent, grant the subject or agent the right to inspect and to receive at reasonable, standard charges for document search and duplication, in a form comprehensible to the subject or agent:
>
> (a) all Personal Information about the data subject, unless otherwise provided by statute, whether the information is a matter of public record or maintained on a confidential basis, except in the case of medical and psychological records, where the records shall, upon written authorization of the data subject, be given to a physician or psychologist designated by the data subject;
> (b) the nature and sources of the personal information, except where the confidentiality of the sources is required by statute; and
> (c) the names and addresses of any recipients, other than those with regular access authority, of Personal Information of a confidential nature about the data subject, and the date, nature, and purpose of the disclosure.

Ind. Code § 4-1-6-3.

> If the data subject gives notice that the data subject wishes to challenge, correct, or explain information about the data subject in the personal information system, the following minimum procedures shall be followed:
>
> (a) the agency maintaining the information system shall investigate and record the current status of that personal information;
>
> (b) if, after the investigation, the information is found to be incomplete, inaccurate, not pertinent, not timely or not necessary to be retained, it shall be promptly corrected or deleted;
>
> (c) if the investigation does not resolve the dispute, the data subject may file a statement of not more than two hundred (200) words setting forth the data subject's position;
>
> (d) whenever a statement of dispute is filed, the agency maintaining the data system shall supply any previous recipient with a copy of the statement and, in any subsequent

dissemination or use of the information in question, clearly mark that it is disputed and supply the statement of the data subject along with the information;

(e) the agency maintaining the information system shall clearly and conspicuously disclose to the data subject the data subject's rights to make a request;

(f) following any correction or deletion of personal information the agency shall, at the request of the data subject, furnish to past recipients notification delivered to their last known address that the item has been deleted or corrected and shall require the recipients to acknowledge receipt of the notification and furnish the data subject the names and last known addresses of all past recipients of the uncorrected or undeleted information.

Ind. Code § 4-1-6-5.

Privacy Awareness

While the State of Indiana's success in the maintenance of individual privacy begins with leadership, all state employees must be aware of and assist with privacy-focused efforts. All state employees should be familiar with this Policy and with the IOT's Information Security Framework. APOs are encouraged to educate employees of their agency regarding applicable privacy statutes and regulations.

Interagency coordination by and between APOs will assist in the State of Indiana's privacy compliance efforts. The CPO can assist APOs as they work to protect the confidentiality of individuals' information.

References

1. *Best Practices: Elements of a Federal Privacy Program*, Federal CIO Council, (June, 2010), https://energy.gov/sites/prod/files/Elements%20of%20a%20Federal%20Privacy%20Program%20v1.0_June2010%20Final.pdf.

Revision History

Version	Date	Name	Revision Description
1	9/15/17	Ted Cotterill	Initial version.

Approval

Chief Data Officer
State of Indiana

APPENDIX D.18
POLICY WORKING GROUP

POLICY WORKING GROUP STRATEGIC PLAN

Chair: Chetrice Mosley | Co-Chair: Tracy Barnes

September 2018
Indiana Executive Council on Cybersecurity

Policy Working Group Plan

Contents

Committee Members **4**
Introduction **7**
Executive Summary **9**
Research **13**
Deliverable: Policy Research Report **16**
General information 16
Implementation Plan 17
Evaluation Methodology 22
Supporting Documentation **24**
IECC Policy Working Group 25

Committee Members

Committee Members

Name	Working Group Representation	Workgroup Position	IECC Membership Type
Lt. Governor Chief of Staff Tracy Barnes	Policy Co-Chair	Co-Chair	Voting
Chetrice Mosley	Policy, Cyber Summit, and Strategic Resources Chair	Chair	IECC Director
John Hammond	Governor's Office	As Needed	Voting
Micah Vincent	Governor's Office	As Needed	Voting Proxy
Superintendent Doug Carter	Government Services Chair	Full Time	Voting
Owen LaChat	Finance Chair	Full Time	Voting
Mark T. Maassel	Energy Chair	Full Time	Voting
John Lucas	Water/Wastewater Chair	Full Time	Voting
Joni K. Hart	Communications Chair	Full Time	Voting
Mark A. Lantzy	Healthcare Chair	Full Time	Voting
Director Danielle Chrysler	Defense Industry Chair	Full Time	Voting
Secretary Connie Lawson	Elections Chair	Full Time	Voting
Secretary Jim Schellinger	Economic Development Chair	Full Time	Voting
Commissioner Fred Payne	Workforce Development Chair	Full Time	Voting
CIO Dewand Neely	PII Chair, Cyber Sharing Chair, Pre- to Post-Incident Co-Chair	Full Time	Voting
Stephen A. Key	Public Awareness and Training Chair	Full Time	Voting
Executive Director Bryan Langley	Emergency Services and Exercise Chair	Full Time	Voting
MG Courtney Carr	Pre- to Post- Incident Chair	Full Time	Voting
Attorney General Curtis Hill	Legal/Insurance Chair	Full Time	Voting
Rhonda Cook	Local Government Chair	Full Time	Voting
Chuck Cohen	Government Services Chair Proxy	As Needed	Voting Proxy
FBI Assistant Special Agent in Charge John Davidson	Government Services Co-Chair	As Needed	Non- Voting

Tom Fite	Finance Co-Chair	As Needed	Advisory
Robert I. Richhart	Energy Co-Chair	As Needed	Voting Proxy
Jon F. Weirick	Water/Wastewater Co-Chair	As Needed	Voting Proxy
Daniel J. Solero	Communications Co-Chair	As Needed	Voting Proxy
Mitchell Parker	Healthcare Chair Proxy	As Needed	Advisory
Jacob Butler	Healthcare Co-Chair	As Needed	Advisory
Kyle Werner	Defense Co-Chair	As Needed	Voting Proxy
Beth Dlug	Elections Co-Chair	As Needed	Voting Proxy
David Roberts	Economic Development Chair Proxy	As Needed	Voting Proxy
Jeff Tucker	Workforce Development Chair Proxy	As Needed	Voting Proxy
Dr. John Keller	Workforce Development Co-Chair	As Needed	Advisory
Ted Cotterill	PII Chair Proxy	As Needed	Advisory
Valita Fredland	PII Co-Chair	As Needed	Advisory
Robert Dittmer	Public Awareness and Training Co-Chair	As Needed	Voting Proxy
Carlos Garcia	Emergency Services and Exercise Co-Chair	As Needed	Advisory
Joe Romero	Emergency Services and Exercise Co-Chair Proxy	As Needed	Advisory
Tad Stahl	Cyber Sharing Chair Proxy	As Needed	Advisory
Ronald W. Pelletier	Economic Development and Cyber Sharing Co-Chair	As Needed	Voting
Col. Jeffery Hackett	Pre- to Post- Incident Chair Proxy	As Needed	Voting Proxy
Douglas Swetnam	Legal/Insurance Chair Proxy	As Needed	Voting Proxy
Stephen Reynolds	Legal Insurance Co-Chair	As Needed	Advisory
Stephanie Yager	Local Government Co-Chair	As Needed	Voting
Scott Miller	Strategic Resources Co-Chair	As Needed	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - National Governors Association Whitepapers
  - State-to-State Examples
  - INSuRE Program (In Progress)
  - Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
  - National Conference of State Legislators Cybersecurity Taskforce Resources and Whitepapers

- **Research Findings**
  - In our research, we were unable to find a comprehensive, deep analysis of federal and state policy around cybersecurity since 2011 which included not just legislation that passed, but legislation that failed as well.
  - The INSuRE project develops a partnership among Centers of Academic Excellence in Information Assurance Research (CAE-R), the National Security Agency (NSA), the Department of Homeland Security, and other federal agencies in order to design, develop and test the research network. INSuRE is a self-organizing, cooperative, multi-disciplinary, multi-institutional, and multi-level collaborative research project that can include both unclassified and classified research problems in cybersecurity.
  - The mission of the National Conference of State Legislators Cybersecurity Task Force is to engage members in policy discussions, educate members and extend networking opportunities to legislative leaders on cybersecurity issues through a series of well-defined programs, webinars on key definitions and critical cyber policy issues as well as supporting private-public networks. The lifespan of this task force would be two years with the option to extend for one additional year.

- **Working Group Deliverable**
  - Complete an analysis of federal policy and state policies related to cybersecurity in the last 5 years.

- **Additional Notes**
  - There is currently Indiana Legislation being proposed (HB1112) that the Policy group is aware. The Council will continue to track this and any additional state legislation that may happen this year.

- **References**
  - Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* - https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
  - INSuRE Program - http://insurehub.org/
  - National Governors Association - https://www.nga.org/cms/home
  - The memo, State Cybersecurity Budgets, provides a brief review of how states budget financial resources for cybersecurity and the current levels of funding in many states.

- **National Conference of State Legislators**
    - Conversation Guide: Executive Branch, Legislative Branch and Higher Education http://www.ncsl.org/documents/taskforces/NCSL_Cybersecurity_Conversation_Guide.pdf
    - Cybersecurity Legislation 2017
    - Data Security Laws for State Government
    - Statewide Chief Information Security Officers
    - Statewide Cybersecurity Task Forces
    - Cyber Education and Training
    - State Cybersecurity Training for State Employees
    - NCSL Law, Criminal Justice and Public Safety Standing Committee Policy on Homeland Security
    - Identity Theft Statutes
    - Security Breaches
    - Cybersecurity Legislation 2016
    - Computer Crime Statutes
    - Data Disposal Statutes
    - Spyware Statutes
    - Phishing Statutes
    - State Efforts to Protect the Electric Grid, April 2016 (NCSL report)
    - "Luring Cybersecurity Is Big Business," Sept. 2015 (article)
    - "States Must Have Cybersecurity Plan," Dec. 2014 (blog post)

- **External Resources**
    - AT&T Security Budget Development (Oct. 31, 2017)
    - The Tech Jobs Conundrum: Tools for Bridging the Confidence Gap (Sept. 2017)
    - Cybersmart Buildings: Securing Your Investments in Connectivity and Automation (Feb. 2017)
    - 2016 National Association of State Procurement Officials Cyber Liability Insurance whitepaper
    - 2016 NASCIO Cybersecurity Study
    - Congressional Cybersecurity Caucus
    - MS-ISAC (Multi-State Information Sharing & Analysis Center)
    - U.S. Department of Homeland Security, Cybersecurity Division
    - "House Set to Push Creation of National Commission on Security, Digital Integrity," Feb. 26, 2016 (blog article)
    - "Administration Announces Cybersecurity National Action Plan," Feb. 11, 2016 (blog article)
    - "What Federal Cybersecurity Legislation Means for the States," Nov. 13, 2015 (blog article)
    - Cyber Supply Chain Security and Potential Vulnerabilities within U.S. Government Networks, June 15, 2015

- **Federal Activities**
    - Cybersecurity Legislation in 115th Congress (March 16, 2017)
    - S. 516 State Cyber Resiliency Act Bill Summary (March 10, 2017)
    - HR 1224 is a new bill on the NIST cybersecurity framework. (March 6, 2017)
    - CISA Law: Section (C) Authorization for Sharing or Receiving Cyber Threat Indicators or Defensive Measures (March 6, 2017)
    - Cybersecurity Legislation in the 115th Congress (March 15, 2017)

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. In Indiana, as state legislation regarding cybersecurity has come up in the last several years, the appropriate state agency has provided resources as needed.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. N/A

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. An education on the topic of cybersecurity with policy makers is needed on a local, state, and federal level.
    b. There are many states that have addressed a variety of cybersecurity topics through legislation. These examples are not easily found collectively and objectively. That is why the IECC is working with partners to conduct primary research and analysis of all state and federal policy that has occurred since 2011.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. N/A

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. The memo, State Cybersecurity Budgets, provides a brief review of how states budget financial resources for cybersecurity and the current levels of funding in many states.
    b. National Conference of State Legislators - http://www.ncsl.org/ncsl-in-dc/task-forces/task-force-on-cybersecurity.aspx

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. National Governors Association Whitepapers
    b. State-to-State Examples
    c. INSuRE Program (In Progress)
    d. Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. The National Conference of State Legislators Cybersecurity Taskforce provides policy makers a variety of resources online.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Complete an analysis of federal policy related to cybersecurity since 2011 and any federal acts that affect cybersecurity today.
    b. Complete an analysis of state policies the last five years that have passed or been debated.

c. Provide as-needed and appropriate input to all policy recommendations presented by other IECC committees and working groups or are being discussed nationwide.
d. Increased understanding and awareness of cybersecurity threats with state and local policy makers.
e. Assist in providing policy guidelines that encourage safer municipality, corporate, and personal practices that protect the state and constituents.
f. Utilize resources allocated to the council for policy tracking and monitoring, especially through university partnerships.

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

a. Help state legislators and local government officials understand and address the growing security risk posed to Indiana and its various sectors.

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. N/A

11. What do we need to do to attract cyber companies to Indiana?

a. N/A

12. What are your communication protocols in a cyber emergency?

a. N/A

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. N/A

Deliverable: Policy Research Report

Deliverable: Policy Research Report

General information

1. **What is the deliverable?**
    a. State and federal research report on cybersecurity legislation

2. **What is the status of this deliverable?**
    a. Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☒ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☒ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable:

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Compiling the policies and legislation that have been introduced since 2011 from all 50 state legislatures and Congress so that Indiana has material and other policies to reference in reviewing policy recommendations.

6. **What metric or measurement will be used to define success?**
    a. Completion of an analysis of all 50 states and federal legislation.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. IECC's committees and members

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None

12. **Who should be main lead of this deliverable?**
    a. IECC Director

13. **What are the expected challenges to completing this deliverable?**
    a. Being able to complete a comprehensive analysis with limited resources and time.

Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability**?
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Select a resource to complete initial research report	Cybersecurity Program Director	100%	January 2018	Selected INSuRE Partner
Conduct research and create a tool to use for future policy analysis	INSuRE Program Partner: University of Alabama	100%	February – April 2018	Cybersecurity Program Director will serve as the Technical Director of the project
Provide Lt. Governor's Office with update on project	Cybersecurity Program Director	100%	March 2018	
Final report and tool completed	INSuRE Program Partner: University of Alabama	100%	April 27, 2018	
Provide IECC with final report and access to tool	Cybersecurity Program Director	0	August 2018	
Update table, additional analysis, and executive summary of changes	IECC approved intern (in-state or public/private partner) or university partnership	0	Once a year	Oversight by Chair and Co-Chair of IECC Policy Working Group
Present IECC with updated executive summary and tool	Cybersecurity Program Director	0	Once a year	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
2.5 FTE	1 FTE	Research and Policy	Grant, public, or private contribution	State of Indiana	The FTEs is expected to be the students to assist with research a few months a year and the Cybersecurity Program Director providing guidance.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Airtable Tool	As the policy collection and sharing grows, there may be a need to add more records beyond the free version and use the advanced features	$10-20 per month depending on upgrade		State of Indiana		

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. As the IECC considers possible policy recommendations, it is imperative that we understand what policy has been discussed, passed, and failed in all 50 states and at the federal level. This will better inform our recommendations, and any that do go before the legislature will likely be more successful because the state will have learned from others. There is no report or tool currently available that comprehensively looks at all cyber policy introduced in all 50 states. This will not only be of benefit to Indiana but other states as well.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. As policy is being discussed, the State of Indiana does not want to pass any legislation that may have an unintended consequence that would increase the cybersecurity risks or impact the investigation of cybercrime. It would be difficult to estimate the costs of the risk reduction.

19. What is the risk or cost of not completing this deliverable?

a. The largest risk of not completing this deliverable is creating a policy that is not well informed, and then unintended consequences occur that would increase the cybersecurity risks or impact the investigation of cybercrime.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion of the policy research will be one metric. Equally important is that the research and possible tool is useful for our policy efforts.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. No state has a publically published review of all cyber legislation introduced since 2011. One could assume those states have had a difficult time moving cyber policy forward, or have not been successful at doing so, and could have benefited from the lessons learned in this type of research project.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. The scope of the project is so large that there is a likelihood that some policies have been missed.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. A resource should be devoted to updating this tool and analysis at least once a year so the information does not become stale and can continue to be useful.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. The Policy Working Group Chair has been working with the INSuRE program to complete the initial report and tool.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All sectors and all committees/working groups.

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. IECC members, IECC leadership, Governor's Office, legislators and their staff, lobbyists, state agency policy directors, sector associations, key national associations, and other state partners

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC and partners will develop a report of state and federal cybersecurity legislation by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- INSuRE Cyber Policy Final Report

IECC Policy Working Group

INSuRE Cyber Policy Final Report

Spring 2018

An Analysis of Cybersecurity Legislation and Policy Creation on the State Level

Adam Alexander aha0007@uah.edu
Paul Graham pag0006@uah.edu
Eric Jackson eaj0010@uah.edu
Bryant Johnson bej0003@uah.edu
Tania Williams tw0063@uah.edu
Cybersecurity Capstone - IS692 - Spring 2018
University of Alabama in Huntsville
301 Sparkman Drive, Huntsville
AL, United States of America 35899

***Abstract* — To best create an effective cybersecurity strategy, it is imperative to understand the policy discussions and trends on a federal and state level. Effective cybersecurity legislation is vital to maintaining our country's infrastructure and protecting our citizenry. Since cybersecurity is often decided on the state level, states need to be aware of the trends in cybersecurity legislation. The purpose of this research was to conduct an analysis of cybersecurity policy from across the United States in an effort to assist the State of Indiana in understanding its cybersecurity risk profile. This analysis included an examination of common trends in cybersecurity legislation. It involved researching cybersecurity policies from all 50 states and the federal government. After creating this baseline, the next phase of the research was to find and record relevant metadata for each policy. This data contained additional data, such as did it pass, who were the supporters, was it revised and other information that is useful to cyber security policy creators. The final goal of the research was to provide a searchable tool that could be utilized to fashion a successful cybersecurity bill and a summary of cybersecurity trends from 2011 to Spring 2018.**

***Index Terms*—cybersecurity, policy, legislation, United States, states, Federal Government**

I. Introduction

A. Problem Statement

It is critical that individual states enact policy dealing with cybersecurity. The National Governors Association, in hopes of addressing the cybersecurity deficit found in states across the nation, drafted A Compact to Improve Cybersecurity. This compact includes a commitment to build cybersecurity governance, to prepare and defend the state from cybersecurity events, and to grow the nation's cybersecurity workforce [1]. However, meeting such a commitment is difficult without an understanding of existing attempts of cybersecurity legislation from across the country.

B. Purpose Statement

In order to assist the State of Indiana in fulfilling this compact by developing their cybersecurity policy, we conducted a policy analysis using the following research questions:

- What policy has been passed successfully/unsuccessfully in other states from 2011 to present?
- Who were the supporters of the policy?
- What type of support did the proposed policy receive, and if it did not pass, why?
- How can such information be presented to Indiana stakeholders in a clear and concise manner?
- What trends are evident among the states regarding cybersecurity policy?

By providing the State of Indiana with a searchable database of successful and failed legislation from across the country, we will supply the state with information needed to create successful and effective cybersecurity legislation.

C. Motivation

As technology advances and cyber threats continue to grow, updating our country's cybersecurity policy is an important and daunting task. Our collective security infrastructure is woefully out-of-date and security policies differ from state to state. Therefore, the governor of Indiana signed executive order 17-11 in January of 2017, creating a council to "develop, maintain and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the strategic vision" of the state [2]. The role of this research was to provide the state with an analysis of existing cybersecurity policy from across the United States proposed from 2011 to present. The research identified trends in policy (whether a policy was adopted or not after proposal). This research will serve as a baseline for the State of Indiana when crafting their policy and will provide valuable insight to other states who might choose to use the research.

Perhaps the greatest concrete problem regarding the research is the scope. It is challenging to do a thorough examination of all the states. We addressed the scope of our work by dividing the workload among the group members.

In order to ensure that all policy was evaluated systematically, we developed a data collection form for the team to use. Additionally, we organized the research by the 20 existing Indiana committees, streamlining the examination and evaluation of the data.

We examined similar trends analysis research and found, while research exists, the scope of the research was narrower. For example, Lowry examined the regulation of mobile payments but only dealt with federal law, making the reporting of such trends much easier [3]. Additionally, we were able to locate studies of trends resulting from one piece of legislations but did not find any previous work dealing with trends regarding state legislation.

We provided a baseline for other large scale legislative trends analysis. Additionally, our database of national cyber-related policies provides a valuable resource for other states as they seek to improve their cybersecurity posture.

II. LITERATURE REVIEW

A. Need for Cybersecurity Legislation

In 2007 the government of Estonia was hit by a cyber-attack that paralyzed the country, shutting down its largest bank, rendering credit cards useless, knocking media outlets offline, and crippling the country's telephone [4]. Could such an attack happen in the United States? Former cybersecurity czar Richard Clarke maintains that "few national governments have less control over what goes on in its cyberspace than Washington" and that "America's ability to defend its vital systems from cyber-attack ranks among the world's worst" [5]. This threat of cyber-attack is not limited the federal government. Individual states also must consider the threat of weak cybersecurity.

States, which hold databases full of health records, driving records, criminal records, professional licenses, tax information, and birth certificates, must have procedures in place to protect this personally identifiable information. The states also often have jurisdiction of cyber-related crimes and are entrusted with cybersecurity education [6]. As Glennon notes, "Every state has enacted laws directed at protecting state governments and businesses specifically from cyber-intrusions" [6]. On top of this, states also bear much of the burden of regulation; however, as Sales states, law and policy of cyber-security are undertheorized and most governments concern themselves with criminal law but are reluctant to see cybersecurity management in regulatory terms [5].

Bosch also notes issues with regulation, stating a reliability standard, such as those created through the Federal Power Act, "does not fully address Smart Grid cybersecurity from an interoperability perspective" [7]. Alternatively, he notes the difficulty of crafting the standards to begin with, citing the failed GRID Act of 2010, which the federal legislative branch could not agree on how the grid's cybersecurity concerns should be addressed [7].

As every state is unique, so must each state take a different approach to cybersecurity. Schneider, in his call for government support of cybersecurity, noted as social values differ, governments should not expect uniform sets of cybersecurity goals; instead "government interventions designed to achieve goals in some geographic region . . . must also accommodate the diversity in goals and enforcement mechanisms found in other regions" [8]. When states craft their cybersecurity legislation is it necessary to build on the experience of other states and to understand national policy trends.

B. Trend Analysis Approaches

As Godara notes, crime has seen a "revolutionary shift from the main actor, the criminal, to certain non-actors in the cyber world called 'intermediaries.' To what extent an intermediary can be held liable for the crimes committed in cyber space is a question which is mooted all over the world" [9]. Godara's research compares legislative and judicial trends in different countries. Her work was limited to rulings regarding intermediary liability in the United Kingdom, United States, and India. When examining legislation in the United States, her approach was to limit her study to federal court cases and sought to analyze fewer than ten rulings.

Bulger, Burton, O'Neill, and Staksrud also examine legislative trends in their examination of how different countries seek to protect children online [10]. In their research, they examined the United States, South Africa, and the European Union. The research targeted key crimes and then reported each country's laws regarding these crimes. Again, the authors chose to research only federal laws and did not examine legislation from individual states.

Neither Godara nor Bulger et al. considered failed legislation when examining these trends [9, 10]. While both research examples relate to trends in cybersecurity, they do not provide an approach to handling the large volume of legislation relating to cybersecurity produced by individual states from 2011 to present.

III. PROGRESS

A. Plan Overview

1) Major Tasks:

- Performed search for state and federal bills.
- Classified state and federal bills.
- Collected metadata and input into collect tool.
- Identified cybersecurity trends from collection tool.
- Created a report detailing trends.

2) Contribution of Tasks to the Overall Utility of the Work: Each task was designed to bring us closer to solving our problem (help the State of Indiana create successful cybersecurity policies). After we classified the state bills, we collected metadata for each one. This task allowed us to

create trends based upon the metadata (passed/failed, detractors/supporters, etc.). Once these trends were identified, then a report was crafted to help committees for the State of Indiana come up with cybersecurity bills that are necessary to protect Indiana's interest and have a higher chance of passing.

3) Deliverables:

- Proposal
- Bi-weekly presentation
- Midterm Presentation
- Midterm Report
- Airtable sortable table with metadata including bill location [https://airtable.com/shrCcYzKJGH1jyvrx]
- Final Presentation
- Final Report

B. Schedule

- 2/1/2018 Met with the technical director and determined goals for the project
- 2/6/2018 Discussed draft proposal with Technical Director
- 2/9/2018 Submitted final proposal
- 2/9/2018 - 3/2/2018 Searched for policies and classification
- 3/2/2018 Prepared midterm report
- 3/2/2018 - 3/23/2018 Completed metadata upload
- 3/24/2018 - 4/13/2018 Identified trends and analysis
- 4/13/2018 - 4/27/2018 Created final report
- 4/27/2018 Submitted final report

C. Detailed Plan

1) Data Collection: After meeting with our technical director, we surveyed academic journals searching for any existing research on the topic. We also reviewed sample legislation, taking note of the metadata provided in the legislation and determining how this data could best be recorded in our database.

After developing a tool for recording pertinent information from state websites, we divided the workload of data collection and started gathering our information.

2) Finding and classifying a bill: Each researcher examined digital archives to look for proposed legislation relating to cyber security. As stated before, each state usually had a digital archive of bills the researcher can look through using a keyword search. Once that location had been exhausted, secondary locations were searched. For each policy found, a certain amount of metadata was located within the policy and recorded. This included the following data:

- Researcher's name (who found the policy)
- Location it belongs to (1 of 50 states, Washington D.C., or the U.S. Congress)
- Type of policy (see classifications below)
- Bill name and/or number
- Source (where the bill can be found)

The included classifications below:

- Government Service
- Finance
- Defense
- Energy
- Water/Wastewater
- Communications
- Healthcare
- Elections
- Economic Development
- Workforce Development
- Personal Identifiable Information
- Public Awareness and Training
- Education
- Emergency Services and Exercise
- Cyber Sharing
- Cyber Organizations (Center)
- Cyber Pre-Thru Post Incident
- Legal/Insurance
- Local Government
- Other critical infrastructure

These classifications were originally the 20 groups that make up the Indiana Executive Council on Cybersecurity and provided an easy way for the end user to reference trends and policies when using the final document as reference. The groups were fine-tuned by the technical director to provide an easier form of classification and more usability.

3) Locating alternative sources for research: Data from primary online sources comprised the bulk of the information collected for the trends analysis. Most states provided some type of searchable archive. However, in cases where such databases were not available, the researchers utilized second party databases to collect policy information. These second party databases included sites such as *Find Law* and *Legiscan*.

4) Creating a collaborative database: While many tools were available for storing and managing our research, we sought one that would allow us to collaborate seamlessly and would allow us to share our data with end users without requiring specialized software or paid licensing. We also sought a product that was versatile enough to allow for linking fields together and even sharing data from one table to another. The tool also needed to have several sorting and filtering options. We found an online product called Airtable to meet our needs [11].

After deciding on a tool, we then had to finetune our database design. We listed the necessary fields and then organized them in a logical way to streamline the data entry process.

5) Importing Database Information: We formatted our information to prepare it for analysis. While reading the bills, the following information was collected in the database:

- Bill number
- State
- Type of policy
- Type of legislation
- Originator (senate, house, joint, or governor's office)
- Year introduced
- Status
- Link to online source
- Related legislation

- Description
- Political party affiliation
- Bill sponsor
- Link to vote count information

6) Trend Analysis: Our next step was to begin the preliminary analysis of our data.

a) By State: Each state had its own cybersecurity policies. The number of each classification for every state was analyzed to discover what was most important to that state. We also made an effort to determine states that were currently active in developing cybersecurity programs.

b) Vetoed Bills: Some states, while successful in passing legislation in the house and senate, failed to garner the support of the state's governor. Since the reasons for such occurrences could be valuable, we wanted to analyze these instances.

c) Failed Legislation: If a certain classification had a high number of bills written but the bills did not pass to become policies, then it can be inferred, while enough people thought the bill would be a good idea, an even greater number of people had negative thoughts about the bill to keep it from passing. This trend was explored to find out why.

d) Influence of Federal Legislation: While states are responsible for crafting their own legislation, we wished to determine if the federal government's actions played a role in determining when and what cybersecurity topics were addressed on the state level.

e) Cybersecurity Pioneers: Cybersecurity is more of a priority for some states than others. By examining the progression of cybersecurity legislation by state per year, patterns showing states who exhibited steady policy creation were evidenced. The states showing consistent policy creation over time were determined to be cybersecurity pioneers.

f) Bipartisan Policy Creation: One of our primary goals in our trends analysis was to determine factors that played a role in the successful passage of legislation. This included the success of a political party in getting a bill adopted. As data collection progressed, it became evident that bipartisan efforts garnered different results than partisan efforts.

7) Analysis of Results: After the trends were examined, then the following questions were addressed.

- Are there states that could be considered pioneers to cybersecurity legislation?
- To what degree does the federal government's actions influence state legislation?
- Are there paths that a bill takes that influences its success?

IV. RESULTS

We identified 500 pieces of legislation relevant to cybersecurity within our eight year sample size. We surveyed 454 policies from all fifty states and Washington, D.C., as well as an additional 46 policies from the federal government.

A. States Currently Active in Passing Cybersecurity Legislation

In order to determine which states are actively developing their cybersecurity program, all 50 states were examined and the number of policies by year were recorded by state, as shown in Figure 1.

Looking at the state policy by year, it was apparent that most states had between 1-10 cyber security policies. There were seven out of fifty states that had 20 or more policies.

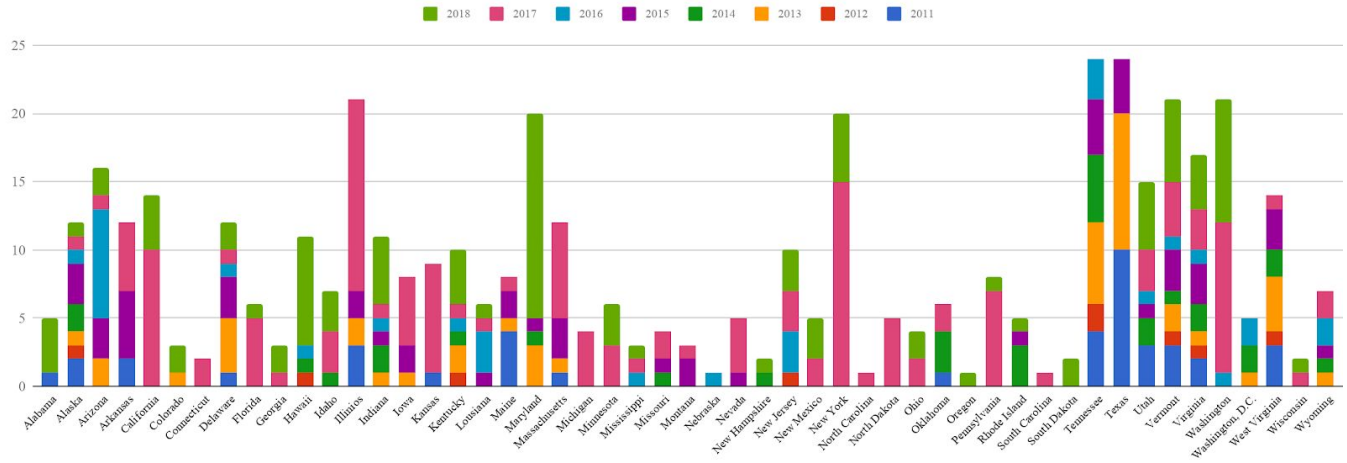


Figure 1. The quantity of policies developed by each state per year between 2011 and 2018.

The dates of the policies were also important. If most policies were proposed before 2016, then the state would not be considered as developing their cybersecurity program. Of the seven states with a large range of policies, only four states created most of their policies from 2016 until now. The four states are Illinois, Maryland, New York, and Vermont.

States with High Number of Policies 2016 - 2018				
Policy Type	**IL**	**MD**	**NY**	**VT**
Communications			5	3
Cyber Organizations	2	1	5	
Cyber Pre Through Post Incident	1	1		5
Cyber Sharing	1	1	3	
Defense		2		
Economic Development		5	5	1
Education	2	3	4	
Elections	1	2	1	
Emergency Services and Exercises			5	
Energy		1	3	3
Finance	1	2		
Government Services	3	2	3	4
Healthcare			1	
Legal/Insurance	3	3	7	5
Local Government	2		2	
Other Critical Infrastructure	1		1	
Personal Identifiable Information			3	4
Public Awareness and Training	1	1	5	
Water/Wastewater			2	
Workforce Development	2	5		
	20	29	55	25

Table 1. The quantity policies and their types that were passed between 2016 and 2018 in the states with the highest surveyed volume.

While a single policy can have multiple policy types, it is still worthwhile to look at the number for each type. Illinois, New York, and Vermont had a high number of legal/insurance policies which would support the argument that most of the new policies being created by developing states were of the type legal/insurance. Vermont also had a high number of government service policies, especially in 2018. Figure 1 shows these two states have a high number of policies spread out over the whole sampling period (2011-2018).

B. Vetoed Bills

In five instances, proposed legislation made it through both the senate and the house; however, the legislation failed to be finalized by a state's governor.

Two of the bills were vetoed by California governor Edmund G. Brown, Jr. Both were introduced in 2017 and were unanimously passed by the state's assembly and senate. Bill AB1306 detailed the scope of the California Cybersecurity Integration Center, which was established by Governor Brown's executive order in 2015 [12]. Brown, in his Governor's Veto Message, expressed concern "that placing the Center in statute as this bill proposes to do, will unduly limit the Center's flexibility as it pursues its mission to protect the state against cyberattacks" [13]. As for vetoed bill AB531, which required the department of technology's office of information security to evaluate existing security policies and develop plans to address deficiencies, Brown stated that the bill's objectives were already required by AB 670 [14].

A bill was vetoed by Governor Susana Martinez from New Mexico. It received 36 to 3 majority votes of support in the state's senate and 37 to 5 majority votes of support in the state's house. HB 364, while dealing primarily with limiting the prescription of contact lenses and glasses, did deal with cyber security by restricting a resident's access to online services. Martinez stated in her House Executive Message No. 57 that the bill limited the use of emerging technologies related to the issuance of contact lenses and glasses [15]. She cited this as the reason she chose to veto the bill.

The other two bills were vetoed by Governor Douglas Ducey of Arizona. Bill SB1434 was vetoed in 2016 after receiving unanimous votes from both the senate and the house. The governor indicated that he vetoed the bill, which dealt with consolidated purchasing and shared services of technology, stating he felt the bill added an extra layer of bureaucracy [16]. HB2566, dealing with password policy, encryption standards, and data security, was vetoed in 2015. It had passed the senate with a vote count of 17 to 11 and passed the house with a vote count of 56 to 1. Ducey stated that his administration had already addressed the concerns outlined in the bill [17].

C. Failed Legislation

Figure 2 shows the twenty classifications used to identify bills and the status count of the policies classification. Although a policy can have multiple classifications, this explores the number of times a classification has a relation to a legislation record.

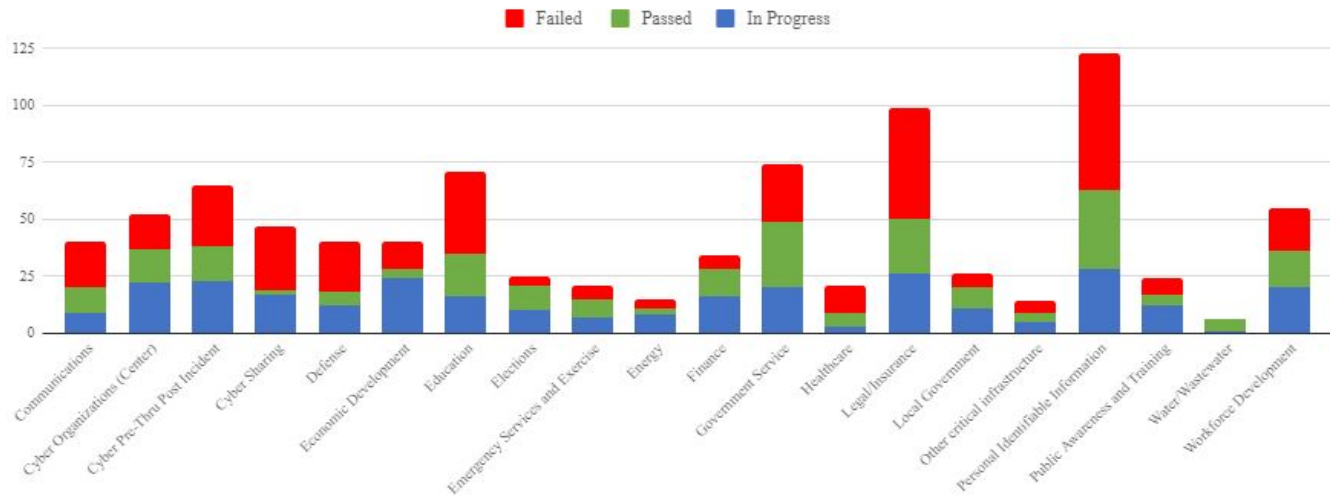


Figure 2. The quantity of each policy type surveyed that is either still in process, was passed into law, or was failed for any reason.

The label "In Progress" are for classifications that are identified to be introduced and still up for discussion, and "Failed" are bills that are inactive, died in chamber, died in committee, or vetoed.

Of the twenty classification types used to identify the bills, most classification types tended to have more failed policies than passed bills. We identified that legislation related to Cyber Sharing, Economic Development, and Education have much higher failure rates than the other classifications. The seven classifications that were an exception include: policies dealing with cyber organizations, elections, emergency services and exercise, finance, government service, local government, and water/waste-water. Furthermore, policies that were related to Elections and Water/Wastewater have greater rates of success than the other classifications. Notably, out of the six state legislations dealing with Water/Wastewater, five were passed successfully, one remains in progress, and zero failed.

D. Influence of Federal Legislation

Figure 3 separates the federal legislation from the state legislation and shows the percentage each topic was covered in bills introduced at those levels within a time frame. In this figure, our eight year sample size was divided into two seperate four year periods to show some slight changes in policy creation.

Much of the federal legislation from the U.S. Congress is focused on Defense, Cyber Pre-through-Post Incident, and

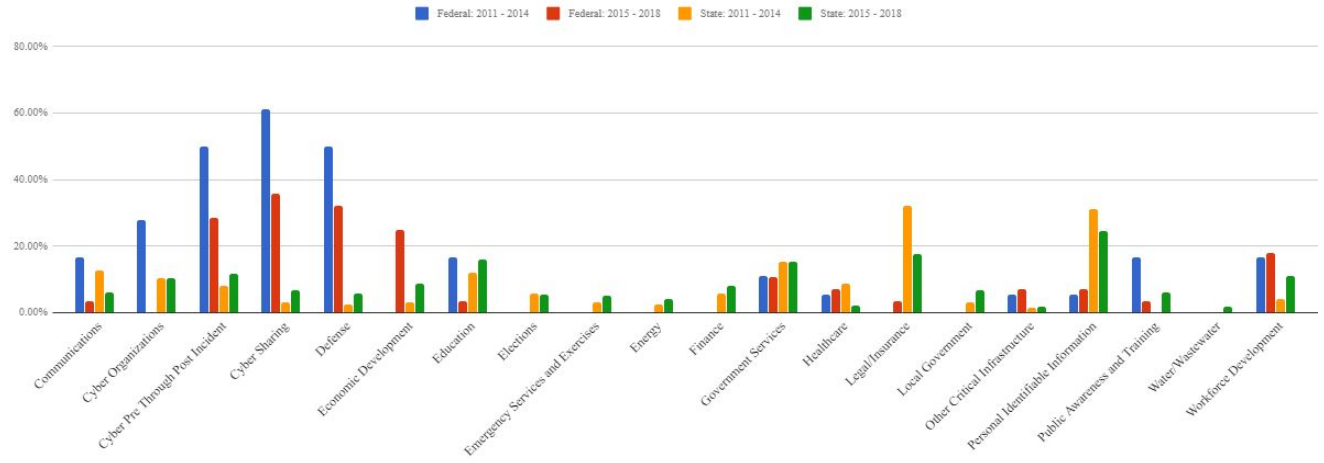


Figure 3. The percentage of state and federal policies introduced in 4 year periods (2011-2014, and 2015-18) that deal each surveyed category.

in Cyber Sharing between organizations. Federal legislation in those categories are consistently higher than all other categories surveyed since 2011. For example, from 2011 to 2014, 61.1% of the federal legislation survey dealt at least some with Cyber Sharing. While those topics were addressed by some at the state level, our data does not show them being addressed by a large amount of states until 2017. Federal legislation appears to be driving state legislation to fill in the gaps where there are security concerns not addressed by the U.S. Congress at all.

In contrast to the federal legislation, state legislation heavily focused on topics such as Education, Personally Identifiable Information, Government Services, Legal/Insurance concerns such as defining cyber security crimes. These were topics that the U.S. Congress did not have many pieces of legislation on at all.

E. Cybersecurity Pioneers

Table 1 shows the number of policies when grouped by state and year. When analyzing the states and the number of policies they have proposed, it is easy to see that most states are not creating new policies. Of the 50 states, only 16 of them have at least 10 new policies since 2011. We used 10 policies as a cut off point since 10 policies provides enough sampling to determine the regularity of policy creation. Pioneering states were Alaska(12), Arizona(16), California(14), Delaware(12), Hawaii(11), Illinois(21), Indiana(11), Maryland(20), Massachusetts(12), New York(20), Tennessee(24), Texas(24), Vermont(21), Virginia(21) Washington(21), and West Virginia(14) These states appear to be in 3 different classifications.

1) Early policy creation; however the state has not produced much legislation of late: In this category, the state created several policies earlier than 2014 and then less after 2014. These states have dropped in their proactive approach to cybersecurity and are not considered as pioneers. For example, Texas created the first bills for various types of policy. While creating several of bills early on, they have not been active in bill creation since 2015. The states of Tennessee, Texas, and West Virginia meet this criteria. Even though their number of policies are high, their concern for cybersecurity seems to have lessened.

2) Large policy creation; however, most of the policies have been created over the last 3 years: This grouping shows states that have created most of their cyber security policies over the past 3 years (2016-2018). These states, while recently producing more legislation, did not have the early policy adoption to be considered pioneers. Arizona, California, Delaware, Hawaii, Illinois, Indiana, Maryland, Massachusetts, New York, and Washington match this criteria. The higher policy producers worth nothing are Maryland (15 policies in 2018 alone), New York (20 policies in the past two years), and Washington (20 policies in the past two years also).

3) Steady policy creation: These high-producing policy creators consistently created bills over the sample years (2011-2018). As they consistently produced more cyber security policies than other states over the same sample time, it would suggest the states were pioneers in cybersecurity policy creation and not as reactive to other states through the years. As Figure 1 "Number of Policies by State per Year" shows, Alaska, Vermont and Virginia are the only states that match this criteria. Vermont has the most policies at 21 followed by Virginia at 17. Alaska did not have near as many with 12.

F. Bipartisan Success

Of the 454 examples of state level cybersecurity legislation found, 109 records were bipartisan attempts. Of those attempts, 29 pieces of joint legislation were listed as actively being considered, meaning the outcome of the legislation was yet to be determined, and 45 of the bills that were introduced passed. When excluding legislation in progress, the resulting bipartisan success rate was 56%. In addition to bipartisan efforts, there were 5 records introduced by council, with all 5 passing. This success rate is significantly higher than partisan sponsored cybersecurity legislation on the state level, where, of the bills that were no longer actively being considered, only 88 passed, indicating a success rate of 40% (see Figure 4).

Cybersecurity topics that garnered the most state level bipartisan sponsorship included those relating to personal identifiable information (22 records), government services (19 records), legal (17 records), and cyber pre through post incident (16 records). There were no examples of bipartisan sponsorship relating to general policies.

Idaho and Kansas were the two states with the most bipartisan sponsored legislation, both having 7 records with bipartisan support. Iowa, Texas, Washington, and Wyoming also were close in this category, having 6 instances each of utilizing bipartisan sponsorship for cybersecurity legislation. States with no bipartisan support of cybersecurity legislation included Arkansas, California, Georgia, Louisiana, Missouri, Montana, New Mexico, New York, North Carolina, Oklahoma, and Wisconsin. Washington, D.C., also had no records in this area.

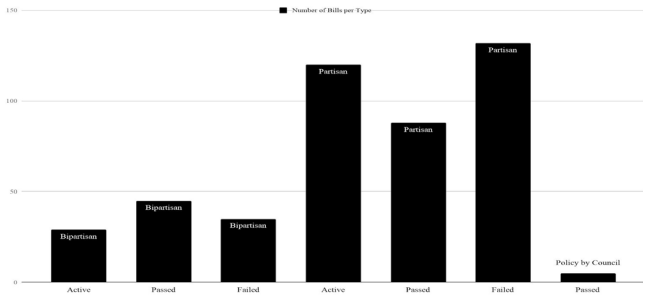


Figure 4. Success of state level bipartisan legislation attempts as opposed to partisan legislation attempts.

This data is being stored at the following link using Airtable. Please follow the link below to view the tool [11].

https://airtable.com/shrCcYzKJGH1jyvrx

V. Challenges

A. Varying Terminology

One problem with our research was how verbiage varied from state to state. For example, one state might choose to use the term *cyber security*, while other states might use terms such as *computer crime* or *online security.* To ensure that each state was researched thoroughly and consistently, the researchers agreed on a list of keywords to use in their search.

B. Determining Relevance

Also, the relevance of the proposed legislation to the targeted analysis data was also a challenge. Desired topics were often buried deep within unrelated information, resulting in researchers having to read and index bills that were, at first glance, not relevant to the desired data set.

C. Tracing a Bill's Origin

Another problem dealt with how bills are created. At times a bill originates in the house, and at other times it can be created in the senate. Bill numbers vary depending on the origin, and they can actually compete with each other. Also, a bill will stall in a committee, or the current legislature may elect not to take up a discussion on the bill. A new bill can be created the following year in order to try to create the policy. These bills must be linked in the research to provide a good picture on policy creation.

Oftentimes a generic bill will pass and become policy. After passing the first bill, a second bill will revise the original policy to provide clarification or additional direction. The original bill and the following bills must be linked in the research also.

VI. Conclusion

Excluding federal legislation and active legislation, we found 305 examples of state level legislation relating to cyber security. Of those, 138 records passed and 167 failed or were determined to be inactive, demonstrating a success rate of 45%.

Policies concerning elections and water/wastewater had higher success rates than other classifications. Policy topics that exhibited higher than average failure rates were related to cyber sharing, economic development, and education.

During the time period sampled, there seemed to be little correlation between federal cybersecurity policy efforts and those of the states. If fact, the two entities tended to complement each other, with federal policy having a much different focus than the states. For example, federal policies dealt more with defense, while state policies dealt more with education.

States showing consistent push in cybersecurity legislation were Vermont and Virginia. These states created policy steadily over the time period and met the criteria to be considered pioneers in cybersecurity legislation.

We determined that one factor that seemed to increase a piece of legislation's chance of success was the willingness of legislators to cross party lines in initiating new legislation. Bipartisan bills had a success rate of 56%, while bills introduced along party lines only had a success rate of 40%. Popular bipartisan topics included personal identifiable information, government services, legal, and cyber pre through post incident. When compared to the overall success rate of 45%. It is evident that bipartisan support is a favorable predictor of a bill's chance of passage.

VII. Future Work

In order for the research to continue to be useful, it is critical that the database be maintained. As new cybersecurity related legislation is proposed and considered, it should be catalogued in the base. By keeping the database current, the picture of national cybersecurity trends will become more granular, and the increased data will allow for better trend analysis.

Additionally, it would be beneficial for future researchers to expand the research by correlating the passage of legislation to related major cyber events. For example, researchers could determine if the Equifax breach resulted in an increase of proposed legislation related to personally identifiable information. If a correlation is evident, this could serve as a predictor of future proposed legislation.

Researchers could also attempt to measure the impact of key successful legislation. An example of this future work could be in the area of workforce development. Researchers could ascertain if states that adopted workforce development legislation have seen an increase in available professionals.

Furthermore, a thorough examination of failed legislation would aid legislators when crafting legislation. By surveying bill sponsors, researchers could identify key barriers to cybersecurity legislation, allowing policy makers the ability to better craft and propose bills. Also, researchers could compare failed legislation from one state to similar successful legislation in another state to determine why similar legislation failed in one state but found success in another.

References

[1] National Governors Association, *Meet the threat: A compact to improve State Cybersecurity*, 2017. [Online]. Available:

https://www.in.gov/cybersecurity/files/NGA%20Cyber%20Compact.pdf

[2] Holcomb, Eric J., "Exec. Order No. 17-11. Continuing the Indiana Executive Council on cybersecurity." *State of Indiana Executive Department*. Jan. 9, 2017. [Online]. Available: http://www.in.gov/gov/files/EO_17-11.pdf

[3] Lowry, C., "What's in your mobile wallet? An analysis of trends in mobile payments and regulation," *Federal Communications Law Journal*, vol. 68, no. 2, pp. 353-384, 2016. [Online]. Available: http://bi.galegroup.com.elib.uah.edu/essentials/article/GALE%7CA493323880/d7c701a94f8c8d9685b93203add71fee?u=avl_uah

[4] Sales, N. A., "Regulating cyber-security," *Northwestern University Law Review*, vol. 107, no. 4, pp. 1503-1568, 2013.

[5] Clarke, R., "War From Cyberspace," *The National Interest*, vol. 104, pp. 31-36. 2009. [Online]. Available: http://www.jstor.org.elib.uah.edu/stable/42897693

[6] Glennon, M. J. "State-level cybersecurity," *Policy Review,* vol. 171, pp. 85-102, 2012.

[7] Bosch, C., "Securing the smart grid: Protecting national security and privacy through mandatory, enforceable interoperability standards," *Fordham Urban Law Journal*, vol. 41, no.4, pp. 1349-1406, 2014.

[8] Schneider, F., "Impediments with policy interventions to foster cybersecurity," *Communications of the ACM,* vol. 61, no.3, pp. 36-38, March 2018.

[9] Godara, S., "Role of 'intermediaries' in the cyber world: a comparative study of the legislative policies & recent judicial trends," *VIDHIGYA: The Journal Of Legal Awareness*, vol. 8, no. 1, pp. 69-80, 2013.

[10] Bulger, M., Burton, P., O'Neill, B., and Staksrud, E., "Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online," *New Media & Society*, vol. 19, no. 5, pp. 750-764. 2017.

[11] Brown, Edmund G. Jr., "Exec. Order No. B-34-15 (2015). Establishing the California Cybersecurity Integration Center," *CA.Gov*, 2015. [Online]. Available: https://www.gov.ca.gov/2015/08/31/news19083/

[12] "State of Cybersecurity," *Airtable* [Online]. Available: https://airtable.com/shrCcYzKJGH1jyvrx

[13] Brown, Edmund G. Jr., "Governor's Veto Message," *California Legislative Information*, Oct. 11, 2017. [Online]. Available: http://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201720180AB1306

[14] Brown, Edmund G. Jr., "Governor's Veto Message," *California Legislative Information*, Oct. 14, 2017. [Online]. Available: http://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201720180AB531

[15] Martinez, Susana, "House Executive Message No. 57," *New Mexico Secretary of State*, Apr. 7, 2017. [Online]. Available: http://sos.state.nm.us/uploads/files/HB364-2017-Vetoed.pdf

[16] Ducey, Douglas A., "Re:Senate Bill 1434," *Office of the Governor*, May 18, 2016. [Online]. Available: https://azgovernor.gov/sites/default/files/sb_1434_veto_letter.pdf

[17] Ducey, Douglas A., "RE: House Bill 2566," *Arizona State Legislature*, Apr. 9, 2015. [Online]. Available: https://www.azleg.gov/govlettr/52leg/1R/HB2566.pdf

TEAM INFORMATION

A. Biographical Sketches

Adam Alexander received his B.S degree in computer science from William Paterson University in Wayne, NJ in 2012. He holds a current Security+ certification. He is in his second year at the University of Alabama in Huntsville (UAH) pursuing a Master of Cybersecurity: Computer Science Track and is set to graduate in May of 2018. Alexander worked for one year as a systems administrator at a software company called Advent. The following three years were spent at MFX Fairfax working as computer technician and eventually being promoted to VDI technician. He has recently interned for TSMO's Army Red team and has participated in several Pen-testing operations.

Paul Graham received his B.S.B.A. degree in management from UAH in 2010. He holds current Security+ and Network+ certifications. He is pursuing a Master of Cybersecurity: Business Track and is set to graduate in May of 2018. Over the last seven years, Graham has worked as a government contractor for the D.O.D. Missile Defense Agency (MDA) in various IT positions. For the last two years, he has been a network design and implementation engineer and collaborated on solutions to improve the MDA's network security posture enterprise-wide. For three years before that, he provided account administration for multiple network domains.

Eric Jackson received his B.S. degree in Computer Science/Software Engineering from the University of Central Florida (UCF) in 2001. He holds a current Security+ certification as well as multiple certifications from Microsoft including Developer of Web Applications, Application Lifecycle Management, and SQL server. He is pursuing a Master of Cybersecurity from UAH with an emphasis on Computer Science.

Jackson worked for a government contractor in Florida for seven years developing simulators for the military. In 2008 he moved to Alabama and has worked as a contractor for NASA since. He is the development team lead, and his duties range from mentoring, server management (IIS), software development/architecture, and interacting with the

customers and government representatives. For the past several years, security has taken a more prevalent role in development. He is responsible for navigating policies, mitigating security scans, and providing a solid framework for use security in the applications.

Bryant Johnson received his B.S. degree in Computer Engineering from UAH in 2016. He also holds a current Security+ certification. He is a CyberCorps: Scholarship for Service student pursuing a Master's in Cybersecurity: Computer Engineering Track at UAH. His experience includes electronics, computer hardware, networking, software design and development.

Currently, Johnson works as a government civilian Computer Engineer for the Aviation and Missile Research, Development, and Engineering Center (AMRDEC) in Huntsville, Alabama, where he performs failure analysis on integrated circuits.

Tania Williams received her B.S. degree in English and professional writing from the University of North Alabama (UNA) in 1994, her Master of Education degree from UNA in 2000, and her Education Specialist Degree in Teacher Leader from UNA in 2015. She is currently pursuing a Master of Cybersecurity from UAH and holds a current Security+ certification.

Williams works for UAH's Center for Cybersecurity Research and Education as a research scientist assisting with the development of cybersecurity curriculum for various cybersecurity camps, including camps at the US Space and Rocket Center (US Cyber) and at UAH (GenCyber). She also is a teacher at Lauderdale County High School, where she teaches cybersecurity, robotics, and English. She is a CyberPatriot coach, a recent Teacher of the Year recipient, and a Fund for Teachers Fellow. Additionally, she has experience teaching on the college level, having served as an associate professor at Northwest Shoals Community college and Faulkner University.

B. Team Tasking

Team members assumed multiple roles to successfully achieve the goals of the project; regular communication of the project's goals was required from all member. Duties included providing expertise, completing deliverables, and documenting the process. While specific tasks varied throughout the course, each person contributed to the overall project objectives by following the outlined detailed plan on assigned datasets:

- Adam Alexander: Alabama, California, Colorado, Connecticut, Delaware, Florida, Georgia
- Paul Graham: Alaska, Arizona, Arkansas, Delaware, Hawaii, Idaho, Indiana, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, U.S. Congress
- Eric Jackson: Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico
- Bryant Johnson: New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota
- Tania Williams: Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming, Washington D.C.

Notably, individuals performed tasks and filled extra roles where responsibility was not specifically dictated. Eric Jackson and Adam Alexander assumed the role of liaisons to the technical director and communicated progress/objectives to the course professor. Tania Williams led the documentation effort, performed the literature review, and established the collaborative database. Paul Graham and Bryant Johnson supported the document review, data management, and analysis.

APPENDIX D.19

PUBLIC AWARENESS & TRAINING WORKING GROUP

PUBLIC AWARENESS AND TRAINING WORKING GROUP STRATEGIC PLAN

Chair: Stephen A. Key | Co-Chair: Robert E. Dittmer

September 2018
Indiana Executive Council on Cybersecurity

Public Awareness and Training Working Group Strategic Plan

Contents

Committee Members **4**

Introduction **6**

Executive Summary **8**

Research **10**

Deliverable: Statewide Cybersecurity Public Relations Plan **13**

General information 13

Implementation Plan 15

Evaluation Methodology 19

Supporting Documentation **21**

ACS Cyberseucrity Guide 22

Deloitte-NASCIO Cybersecurity Survey 95

Global Cyber Security Capacity Centre Cyber Security Awareness Campaigns "Why do they fail to change behavior?" Draft Working Paper 132

IECC Public Awareness and Training Working Group Public Relations Plan 2018-2020 171

ITU Cybersecurity Index 228

Pew Research Center What Americans Know About Cybersecurity 307

Committee Members

Committee Members

Name	Organization	Title	Committee/ Workgroup Position	IECC Membership Type
Stephen A. Key	Hoosier State Press Association	Executive Director	Chair	Voting
Robert E. Dittmer	REDCOM Public Relations Consulting	President	Co-Chair	Voting Proxy
David Hosick	IN Dept. of Homeland Security	Communications Director	Full Time	Advisory
Nicole Needham	IN Office of Technology	Security Awareness Manager	Full Time	Advisory
Graig Lubsen	IN Office of Technology	Director of Communications	Full Time	Advisory
Julie A. Vincent	IUPUI	Public Relations Lecturer	Full Time	Advisory
Brian O'Hara	InfraGard	Past - President	As Needed	Advisory
Greg Ellis	Indiana Chamber of Commerce	VP, Energy and Environmental Policy	As Needed	Advisory
Dave Arland	Indiana Broadcasters Association	Executive Director	As Needed	Advisory
Kathleen Johnston	NA	Media Freelancer	Full Time	Advisory
David Woodward	Indiana Department of Education	Director, Building Security and Safety	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - The Public Awareness and Training Working Group (PATWG) has submitted questions to all IECC committees/work groups to help determine the needs of those units. PATWG received a proposal from Julie Vincent's J428 Public Relations Strategic Planning and Research class at IUPUI with outreach plan for citizens and high school students. PATWG also reviewed a study released by the PEW Research Center on March 2017, which is titled "What Americans Know About Cybersecurity.

- **Research Findings**
  - Comprehensive plan for public awareness and training will have two distinct components: one geared toward the public at large and another tailored for the specific needs of other IECC committees and work groups. Any plan will require the state to commit resources for implementation.

- **Working Group Deliverable**
  - Statewide Cybersecurity Public Relations Plan

- **Additional Notes**
  - Next step for PATWG is to reach out personally to other committees/work groups through script prepared by co-chair Bob Dittmer to supplement written responses to work group's questions. The needs analysis will help PATWG create the comprehensive plan.

- **References**
  - [No Response]

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. There has essentially been no coordinated statewide effort to educate the general public about cybersecurity efforts. Individual industries and individual state agencies have conducted various programs focused generally in areas of their responsibility. The Indiana Attorney General has conducted a limited campaign, and the Indiana Office of Technology (IOT) has extensive training opportunities available and has worked in a limited fashion to promote cybersecurity awareness. Department of Revenue (DOR) has worked to educate taxpayers on fraud prevention.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. The greatest vulnerability is the general lack of both awareness and knowledge among the general public on how best to protect themselves from cyber attacks.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Public knowledge gap.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. None.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Very few. Virginia has done some work in this area and will be used as an initial model. However, they have no cohesive, comprehensive plan.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. PEW Research Center study: "What Americans Know About Cybersecurity." Conducted June 2016; Published March 2017.
    b. "ACS Cybersecurity: Threats, Challenges, Opportunities." Australian Computer Society, November 2016.
    c. "Cyber Security Awareness Campaigns: Why do they fail to change behavior?" draft working paper, Global Cyber Security Capability Center, July 2015.
    d. IUPUI student survey (convenience sample) conducted of Indiana residents, November 2017.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Governor's Association and selected (few) states. Individual Indiana state agencies with limited perspectives and individually focused activities.

8. **What does success look like for your area in one year, three years, and five years?**
    a. One year:
        i. Achieve awareness of cybersecurity protective measures to 50 percent of Hoosiers.
        ii. Achieve active Cybersecurity activities by Hoosiers to 25 percent.
        iii. Achieve 20 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
    b. Three years:
        i. Achieve 80 percent awareness of cybersecurity protective measures by Hoosiers.
        ii. Achieve 50 percent active cybersecurity protective measures by Hoosiers.
        iii. Achieve 50 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
    c. Five years:
        i. Achieve 90 percent awareness of cybersecurity protective measures by Hoosiers.
        ii. Achieve 75 percent active cybersecurity protective measures by Hoosiers.
        iii. Achieve 75 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. N/A

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. N/A

11. **What do we need to do to attract cyber companies to Indiana?**
    a. N/A

12. **What are your communication protocols in a cyber emergency?**
    a. N/A. See procedures for Indiana Joint Operations Center and Joint Information Center.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. From a public awareness and training perspective, there are none. See Supporting Documentation.

Deliverable: Statewide Cybersecurity Public Relations Plan

Deliverable: Statewide Cybersecurity Public Relations Plan

General information

1. **What is the deliverable?**
    a. The PAT working group will create an initial public communication plan for execution in two phases. The first phase will educate Hoosiers about cybersecurity and high schools students about cybersecurity careers. The second phase will be focused on supporting awareness and cyber defense for specific industries and businesses (working with all other committees and working groups).

2. **What is the status of this deliverable?**
    a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**

    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**

    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Initial deliverable will be a complete cybersecurity public awareness campaign plan that is designed to increase public awareness and knowledge about methods to protect individuals and systems from cyberattack. A second level plan will target businesses and industries to build awareness and knowledge. Both will include communication planning to change physical behaviors to enhance cybersecurity by individuals and employees/businesses.

6. **What metric or measurement will be used to define success?**
    a. A series of measurable awareness, knowledge and behavior traits will be used for measurement.

7. **What year will the deliverable be completed?**
    a. 2018
    b. Note: the plan will be delivered in 2018. However, execution will be a multi-year activity.

8. **Who or what entities will benefit from the deliverable?**
    a. All Hoosiers and Hoosier businesses.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. While there are some individual and limited state departments promoting good cybersecurity habits, research would suggest there is no entities taking a holistic approach to the problem. This will be that approach.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. We will be working with all other committees and working groups to develop the second phase of the communication plan targeting behaviors of employees and businesses.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Federal agencies: none
    b. State agencies: perhaps all, perhaps none. Most likely, however, IOT and Department of Homeland Security (DHS) along with the Governor's office.
    c. Associations: Probably many industry and trade associations will need to be involved.
    d. Non-profit organizations: Unknown at this time.

12. **Who should be main lead of this deliverable?**
    a. Governor's office or identified lead agency. Could be IDHS or IOT.

13. What are the expected challenges to completing this deliverable?

a. If the deliverable is the plan, none. However, implementation will require funding and/or staffing.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Plan	Working Group	100%	May 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
At least one	At least one	Senior Public Relations Professional	Appropriated	None	At least one very experienced public relations professional working from the Governor's office with overall responsibility for plan execution, public representation, and coordination among key agencies. Will also oversee activities and budget for advertising agency.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Advertising and creative agency	Advertising portion of the campaign plan requires development of print, online and broadcast advertising	SWAG: $250,000.00	SWAG: $250,000			
Purchase of advertising space	Support of campaign; broad reach; message consistency	Incl.	Incl.			

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Principle benefit is a coordinated approach to increasing public awareness of the need for cybersecurity awareness, knowledge, and activity across all key constituent groups, but especially the general public.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. The more active the public is in defending personal and business systems from cyberattack, the less risk to individuals, businesses, and the state's critical infrastructure.

19. What is the risk or cost of not completing this deliverable?

a. The risk is status quo: where there is measurable ignorance of cybersecurity and even less individual cyber defense activity exposing the State's people and infrastructure to potential compromise.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Metrics are included in the plan. Principle baseline of measurement is a Pew Center Study from 2016.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No
b. **If Yes, please list states/jurisdictions**
   i. Not recommended. Measure against a national standard (Pew Study).

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. Every state. But, not recommended.
    ii. We can examine using Ohio or Illinois or Kentucky. The challenge will be conducting sufficient research to measure their lack of activity and results.
    iii. In this case, it is more important to measure against a national standard (the Pew Study) than comparing to individual states.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Budget availability
b. Personnel availability

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Continued support for qualified personnel and a supportive budget.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Currently working with the Cybersecurity Program Director.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. It is intended to continue this planning process to include activities support each of the other sectors as their operational plans become more defined. This planning will likely take place during the first phase (year 1) of the plan and be executed in the second phase (years 2-3).

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Cybersecurity Council
b. Governor
c. Senior agency leadership

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. No

30. What are other public relations and/or marketing considerations to be noted?

a. N/A

Evaluation Methodology

Objective 1: The IECC Public Awareness and Training Working Group complete a statewide public relations cybersecurity campaign plan by June 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC will implement an IECC public relations micro-plan on year one efforts by September 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- ACS Cybersecurity Guide
- Global Cyber Security Capacity Centre: Cyber Security Awareness Campaigns "Why do they fail to change behavior?" Draft Working Paper
- Deloitte NASCIO Cybersecurity Survey
- IECC Public Relations Plan
- ITU Cybersecurity Index 2017
- Pew Research Center – What Americans Know About Cybersecurity

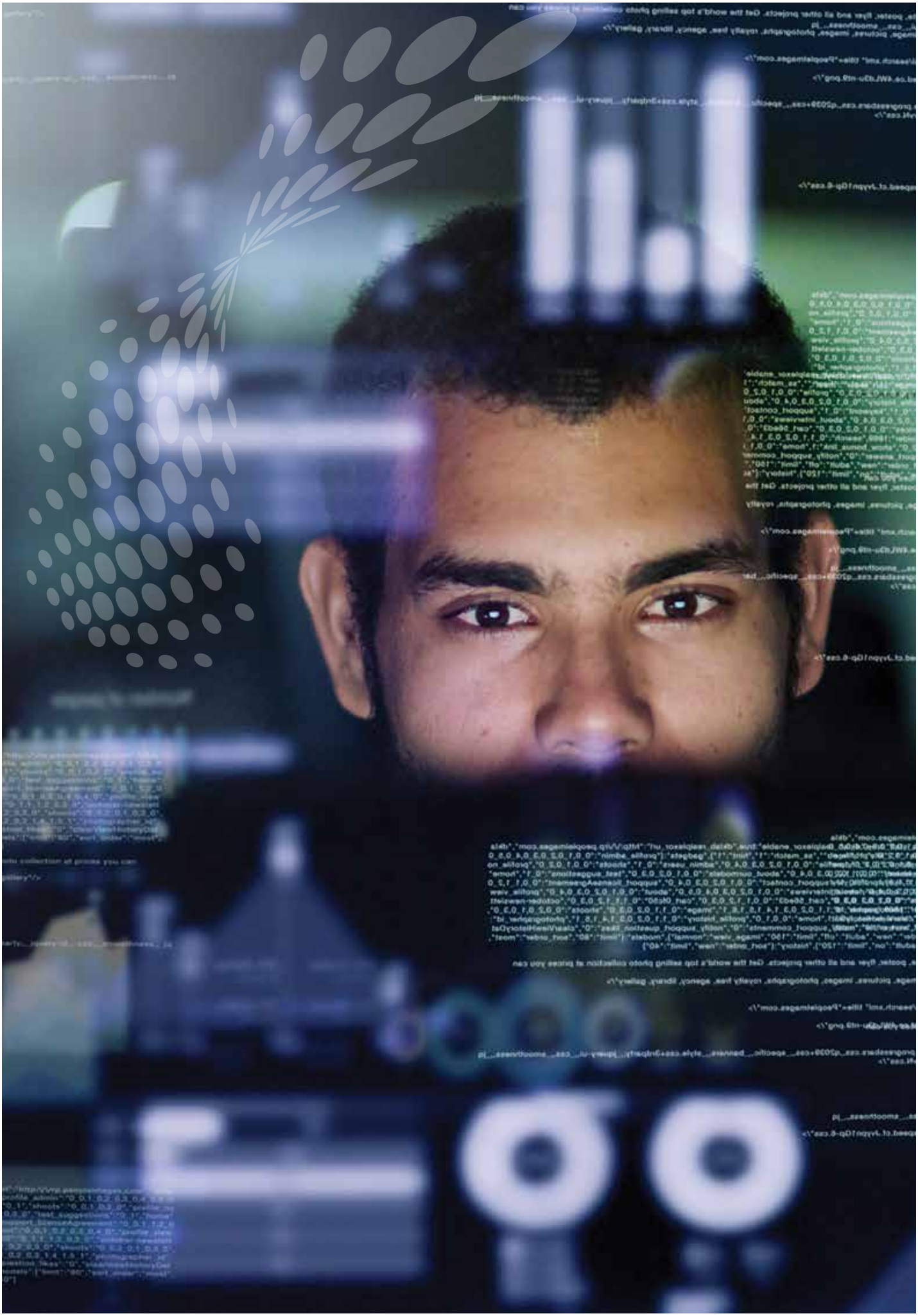
ACS
Cybersecurity Guide

November 2016

November 2016

Cybersecurity

Threats
Challenges
Opportunities



“It is only when they go wrong that machines remind you how powerful they are.”

Clive James

Contents

01

Foreward 1

Executive summary 4

02

A brave new world 5

Cyber speak! 6

What is cybersecurity? 7

And the weakest link is... 9

A world without cybersecurity 11

03

Threats in the information age 13

The nature of threats 14

The Internet of Things (IoT) 16

Botnet armies 17

When security is an afterthought 18

Autonomous systems 19

Driverless cars and transport 19

ATMs and Point of Sale 21

What about wearables? 22

Cyberwarfare 24

Automated attacks 24

Energetic Bear 24

Cyberattacks on infrastructure 26

When software kills 28

Data manipulation 29

Backdoors and espionage 29

Cloud concerns 29

Blast from the past 30

Virtualised threats 32

Industry and the individual 33

Ransomware and Cryptoware 33

Multi-vector attacks 33

Identity theft 34

The world we live in 34

04

The future in our hands 35
The 100% secure computer 37

Opportunities 38
The data-driven economy 38
Technology as wealth creation 39
Cybersecurity as job growth 39
Leveraging technology talent 39

Challenges 40
Leadership 40
Learning from history 40
Collaboration 41
Education and awareness 41
You are what you do 43
Legal and regulatory 43
Services and privacy 43
Perception and practicality 44

05

Looking to the road ahead 45
State of the nation 46
What role can you play? 47
Government 47
Education and research 50
Business and industry 50
You, the individual 50

The five pillars of cybersecurity readiness 51
Online resources 52

Through the looking glass 53
Fast facts 55
Glossary 57
References 59

Foreword

You've seen documents like this pass your desk before, but we hope this one is a little different. You can gloss over it, seeking the diamonds in the rough, but take the time to delve into the information presented here and you will walk away with a different appreciation of the laptop on your desk, the car that you drive, and the phone that you carry.

Protecting that upon which we depend should be front of mind for government, business and industry, academia and every individual with a smartphone in their pocket.

Not to mention the planes you fly, the banks that hold your money, the hospitals that keep you alive and the very infrastructure that makes our cities run. In short: the basis of our modern lives.

It can be hard to not overuse a word that's become popular thanks to public awareness, but 'cyber' is now firmly entrenched in our language and our mindset, by virtue of the fact that our society today depends so much on technology.

So we're going to talk about cyber with respect to security, as the two are intimately intertwined. In this guide we aim to break down what is sometimes a large and complex issue into an easy to read and digestible summary that should – if we've done our job well – give you the tools to both talk confidently about the issues, as well as equip you with the core information required to make decisions around cybersecurity.

Because, despite the technical nomenclature, the issue of cyber-security is as vital to our way of life as technology itself. In fact, they can't be separated: our economic health, our national security, and indeed the fabric of our society is now defined by the technology we depend on every day.

What's left unsaid here, however, is the assumption that this technology will continue to work as we intend – but this is only true if we can protect it from being hacked, manipulated, and controlled.

Logically, then, protecting that upon which we depend should be front of mind for government, business and industry, academia and every individual with a smartphone in their pocket.

Which is to say, all of us.

If you are part of government, this primer serves as a guide to the greater sphere of cybersecurity and how it relates to our national security, our national interest, and our economic prosperity.

If you are an executive, board member, business leader, or IT professional this is an opportunity to verse yourself in the language and the ecosystem, the threats and the opportunities, and to better communicate the issues and responsibilities around cybersecurity within your organisation.

And if you are simply an individual interested in understanding more about the nature of our digitally-driven world, this guide will provide the basics and a clear overview of how cybersecurity relates to you.

At the ACS we welcome every opportunity to educate and assist. If you have any questions, or would like more information, please feel free to contact me at: anthony.wong@acs.org.au.

Enjoy this guide. We hope it will make a difference to you.

Anthony Wong
President, ACS

SECURING AUSTRALIA'S FUTURE

At ACS we are passionate about the ICT profession being recognised as a driver of productivity, innovation and business – able to deliver real, tangible outcomes.

This year ACS celebrates 50 years of advancing ICT in Australia. Our founders and pioneers worked on the first innovative computers in government, academia and industry, and our members now work at the coalface of technology development across every industry.

In 2011, ACS brought together its own Cyber Taskforce from our 23,000 members to respond to the Federal Government's new cyber discussion paper, 'Connecting with Confidence', where we highlighted the need to develop co-ordination and a focus on the pipeline of cyber professionals.

To play our part in securing Australia's future, we continue to perform the role of trusted advisor to government, and deliver services to identify and certify ICT professionals you can trust, including through the Professional Standards Scheme that assures professionals have the specialist skills business can rely upon.

ACS is part of the global federation of professional ICT societies, the International Federation for Information Processing (IFIP), and the first professional body to receive accreditation under the International Professional Practice Partnership (IP3) – providing a platform for accreditation for ICT professionals and mutual recognition across international boundaries. The ACS currently chairs IP3 and plays a leading role in the professionalism of the ICT workforce.

IP3 has since gained global attention after successful engagements at the World Summit on the Information Society (WSIS) Forum in Geneva and the United Nations in New York, where the importance of ICT professionalism was acknowledged by the UN General Assembly President in 2015.

In May 2016 the President of IFIP participated in the European Foresight Cyber Security Meeting where he advocated that professionalism of the ICT workforce is "a key element in building trustworthy and reliable systems" and that it is important to ensure that "cyber security and cyber resilience is also a duty of care of the individual ICT professional".

As we move forward another 50 years, ACS will be there at the forefront meeting the challenges and opportunities of ICT, and supporting the growth and potential of ICT professionals in Australia.

01

Executive summary

As technology continues to evolve so also do the opportunities and challenges it provides. We are at a crossroads as we move from a society already entwined with the internet to the coming age of automation, Big Data, and the Internet of Things (IoT).

But as a society that runs largely on technology, we are also as a result dependent on it. And just as technology brings ever greater benefits, it also brings ever greater threats: by the very nature of the opportunities it presents it becomes a focal point for cybercrime, industrial espionage, and cyberattacks. Therefore, protecting it is of paramount priority.

This guide looks at some of the concerns facing us in the near future that include:

- Attack vectors such as botnets, autonomous cars and ransomware.
- Threats including data manipulation, identify theft, and cyberwarfare.
- Tangential issues such as data sovereignty, digital trails, and leveraging technology talent.

Additionally, it provides some background to the nature of digital ecosystems and the fundamentals of cybersecurity.

Critically, this document clarifies the importance for Australia to take responsibility for its own cybersecurity, especially with regards to essential infrastructure and governance.

On the flip side – and as one of the fastest growth industries globally – developing our own cybersecurity industry is also an opportunity for economic growth, job creation, and education – ensuring Australia is well positioned for a future as a digitally advanced nation.

Finally, we look at some of the challenges that countries worldwide are currently dealing with in regards to cybersecurity, including:

- The need for more collaboration in order to mitigate threats.
- Education and awareness; and
- The balance between privacy and security.

Our aim is that this document provides an informative primer on the relevant issues facing Australia in relation to cybersecurity, to generate discussion and debate, and to raise awareness with regards to a fundamental building block of the technologically-dependent society which we have already become.

As you will read in the following pages, cybersecurity is not optional. It must form part of the design of every product, of every database, of every electronic communication. And – through education, awareness, and proactive change – we can all play a part in securing our future.

A brave new world

You're reading this document written with, laid out by, and printed using computers. From start to finish it existed as 0s and 1s – the binary blood of our modern world.

In fact, our lives today are codified by data: almost everything we do, and everything we depend on, involves data and the technology that uses it – there are scant few areas not touched by this revolution we call the **information age**.

CYBER SPEAK!

Every industry has its own lexicon, and the cyber world is no different. While built on technological foundations that we all know – computers, the internet, smartphones, and similar – as you delve deeper into the subject you start to encounter acronyms and technical concepts that you may not be familiar with.

And, if we're all to communicate on the subject of cybersecurity – across all sectors of government, business, industry, and academia – then it can help to familiarise yourself with the nomenclature associated with this diverse and compelling subject.

To this end we've included a Glossary on page 57. Feel free to flick back and forth as you read to ensure you get the most out this document, spending more time expanding your knowledge and less time scratching your head!

And so it follows that in order to keep our way of life – and to continue to prosper through technology – we must ensure that it always operates and works for us as intended.

And for the most part it does, until it's hacked. In the hands of less than favourable individuals, organisations, and governments, technology and the data it depends on can be turned against us.

When you read yet another report of a multimillion-dollar bank theft, yet another million usernames and passwords leaked on the web, or yet another scam milking millions from vulnerable people – what you are reading about is the lack of cybersecurity: a failure to protect systems, processes, or data and thereby enabling exploitation. Sometimes the end result is just an embarrassment for a company or individual; at other times it can cause significant financial or operational harm. At its worst, loss of life can be a result.

Cybersecurity, then, is not optional. As our world transitions more products and services online, and we in turn depend on them, protecting this technological infrastructure has become a fundamental building block for information systems globally. It must underpin every technology, every gadget, every application, and anywhere data is stored.

To help understand the risks, this document will explore the threats Australia faces in this digital age: to our economy, our sovereignty, and ultimately, our way of life.

It will also cover the opportunities as a burgeoning industry – one that is projected to be worth $US639 billion[1] globally in the next seven years alone – and the possibility for Australia to establish itself as a leader, pioneering new technologies and exporting cybersecurity products to the rest of the world.

We are more than just the lucky country. We are early adopters. We are tenacious innovators. We are a nation with the skills and talent to lead the world in cybersecurity – and with the right mix of leadership and commitment from government, industry, and academia, we can make it happen.

What part will you play?

46%

OF THE WORLD'S POPULATION IS CONNECTED TO THE INTERNET

What is cybersecurity?

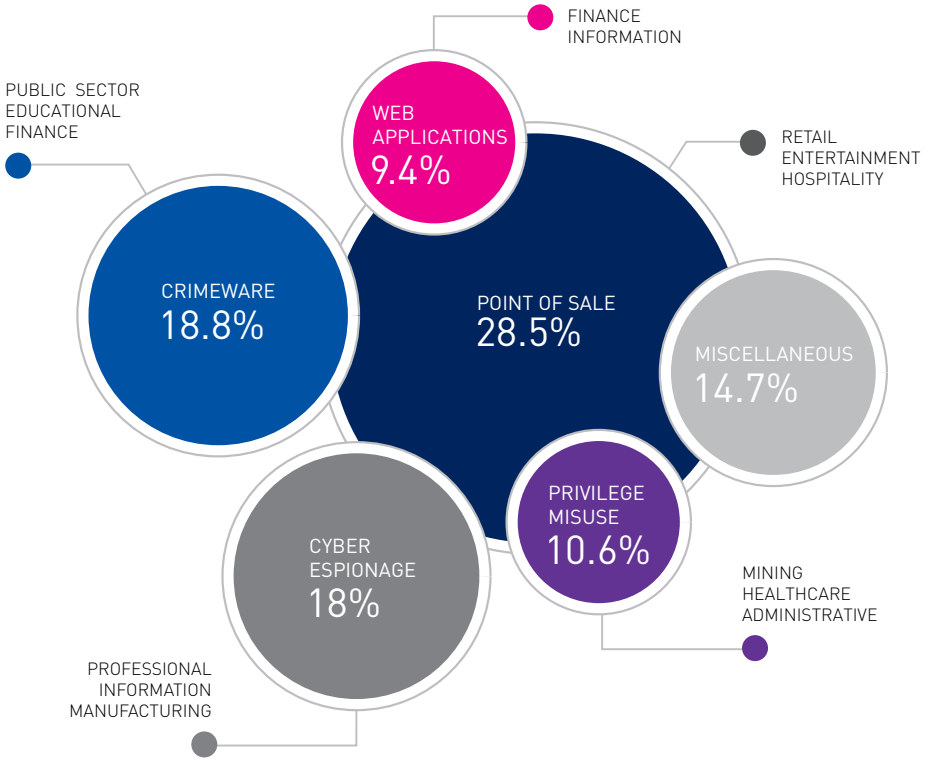
As with any technological advance throughout history, whenever new opportunities are created, there will always be those that exploit them for their own gain.

Despite the threat of viruses and malware almost since the dawn of computing, awareness of the security and sanctity of data with computer systems didn't gain traction until the explosive growth of the internet, whereby the exposure of so many machines on the web provided a veritable playground for hackers to test their skills – bringing down websites, stealing data, or committing fraud. It's something we now call **cybercrime**.

Since then, and with internet penetration globally at an estimated 3.4 billion users (approximately 46% of the world's population[2]), the

THREAT VECTORS BY INDUSTRY

The vectors by which industries are compromised.
Source: Verizon 2015 Data Breach Investigations Report



opportunities for cybercrime have ballooned exponentially.

Combating this is a multi-disciplinary affair that spans hardware and software through to policy and people – all of it aimed at both preventing cybercrime occurring in the first place, or minimising its impact when it does. This is the practice of **cybersecurity**.

There is no silver bullet, however; cybersecurity is a constantly evolving, constantly active process just like the threats it aims to prevent.

What happens when security fails? While what frequently makes the news are breaches of user accounts and the publication of names and passwords – the type that the Ashley Madison hack publicly exemplified – it's often financial gain, or the theft of critical business or government intelligence, that drives the cyber underworld.

One fact remains clear: it's only going to increase. As we integrate technology further into our lives, the opportunities for abuse grow. So too, then, must the defences we employ to stop them through the education and practice of cybersecurity.

The increasing prevalence and severity of malicious cyber-enabled activities... constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States. I hereby declare a national emergency to deal with this threat.

Barack Obama,
President of the United States, 2015[3]

LAST
TO KNOW

MORE THAN
90%
OF BREACHES ARE DISCOVERED BY EXTERNAL PARTIES

WHAT'S THE PASSWORD?

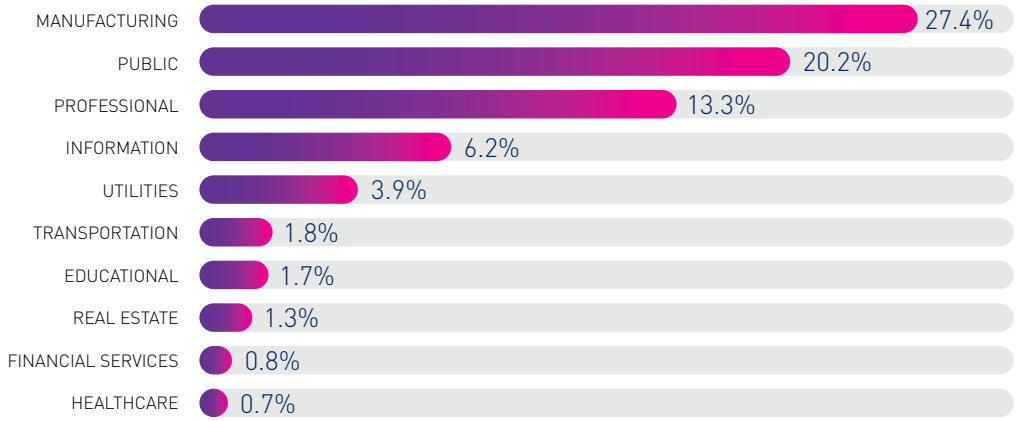
63%
OF BREACHES ARE CAUSED BY WEAK, DEFAULT, OR STOLEN PASSWORDS

EASY HACKS, EASY BREACHES

Source: Verizon 2016 Data Breach Investigations Report

TOP 10 ESPIONAGE TARGETED INDUSTRIES

The most targeted industries in 2015.
Source: Verizon 2015 Data Breach Investigations Report



AND THE WEAKEST LINK IS...

Humans are inherently complex and multi-faceted creatures with our own agendas, influences, faults, beliefs, and priorities.

Sometimes we're also simply just too trusting.

Even the most hardened system can be breached through **social engineering** – the 'hacking' of people. No amount of secure network topologies and firewalls or security software can withstand a user innocently clicking on an email link, or being convinced to give up login details over the phone by someone pretending to be from the IT department.

In fact a recent study by researchers at the Friedrich-Alexander University of Erlangen-Nuremberg, Germany, revealed that just over 50% of people click on links in emails from strangers, **even when they were aware of the risks**.[4]

And so, as a result, cybersecurity isn't just about technological defences: it's also about people. From the home user through to industry and government, everyone needs a basic understanding of cyberthreats and how to recognise them – something which comes under the umbrella of **digital literacy**.

A world without cybersecurity

93% OF CASES HACKERS TOOK JUST MINUTES TO BREACH | WHILE COMPANIES TOOK WEEKS OR MONTHS TO DISCOVER

SHOW ME THE MONEY | 95% OF WEB ATTACKS ARE FINACIALLY MOTIVATED

EMPLOYEE MISTAKES | LOST ASSETS 100x TIMES MORE PREVALENT THAN THEFT

NEARLY 30% OPEN PHISHING EMAILS | 12% DO CLICK THE LINK OR OPEN ATTACHED FILES

SIMPLE MISTAKES, COSTLY LOSSES
Source: Verizon 2016 Data Breach Investigations Report

One the most damaging targets for a society embroiled in cyberwarfare is infrastructure.

Our reliance on automation focuses single points of failure that can have dramatic consequences if directed at power stations, communication networks, transport and other utilities.

By way of example, and to draw from the emerging technology of driverless cars gaining popularity now, is the following example of what might happen if we continue to create products and services without cybersecurity in mind:

Thirty years from now our society runs on automated cars, buses and trains. Planes still require human authority – for now – and drones line the sky. On the one hand, this advance in technology has brought much greater efficiency: traffic jams eliminated, pollution lowered, cheaper cost of transport and more. It's a golden age.

Then a cyberattack compromises the central network. The systems that co-ordinate all transport shut down, bringing the city of Sydney – now 7 million people – to an abrupt halt.

No cars, no buses, no trains.

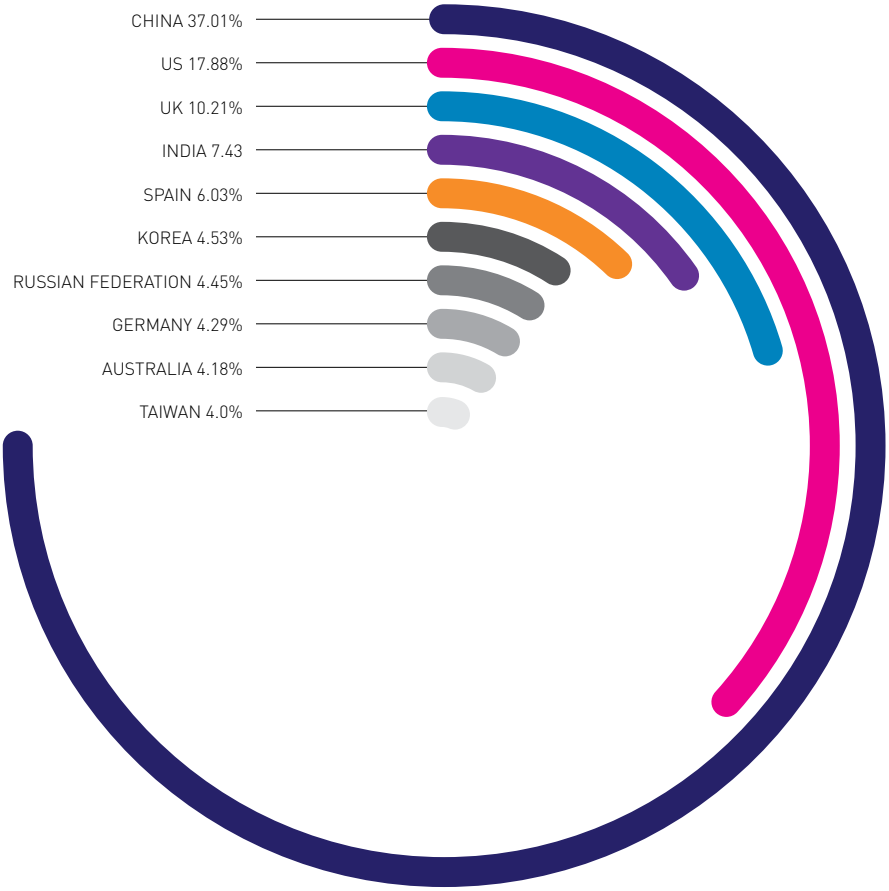
Workers can't get to and from work, and productivity stops. Life-saving medicine doesn't arrive and people die. Essential services begin to fail, and chaos ensues. The economic and social fallout is immense: a city held hostage by an external force – be it terrorist, criminal, or foreign power. Australia invaded without the invader ever stepping on our shores.

It's a stark example, but it demonstrates the Achilles heel the inter-connected society that we are heading for right now, and the reason cybersecurity must be part of all technology from the outset.

Consider this: the internet has enabled entirely new business models that have already shaped our planet. But the Googles and Facebooks and Amazons of this world are not the most profitable organisations that conduct business over the internet today – that crown belongs to cybercrime. It speaks volumes that the most lucrative business on the internet today is fraud.[9]

Q2 2015 saw one of the highest packet rate attacks recorded... which peaked at 214 million packets per second (Mpps). That volume is capable of taking out Tier 1 routers, such as those used by Internet service providers (ISPs).

Akamai, State of the Internet Q2 2015 Report[10]



TOP 10 SOURCE COUNTRIES FOR DDOS ATTACKS, Q2 2015

Top sources of mitigated DDoS attacks on Akamai's network.
Source: Akamai State of the Internet Report, Q2 2015

Threats in the information age

Every minute, we are seeing about half a million attack attempts that are happening in cyberspace.

Derek Manky,
Fortinet Global Security Strategist[5]

500 Thousand

500,000 ATTACKS AGAINST FORTINET EVERY MINUTE

To understand just how technology becomes vulnerable to cybercrime, it helps to first understand the nature of threats and how they exploit technological systems.

You might first ask why technology is vulnerable at all, and the answer is simple: trust. From its inception, the protocols that drive Internet, by and large, were not designed for a future that involved exploitation – there was little expectation at its birth that we might need to one day mitigate against attacks such as a **distributed denial of service** (DDoS), or that a webcam you buy off the shelf might need security protocols to prevent it being hacked and used to spy on you.

There is much greater awareness today, but even so you can still buy devices that connect to the internet that have poor security measures or no security at all built-in, because up until recently this simply wasn't part of the design scope. In many cases, the idea that a device might be used for nefarious purposes isn't even considered.

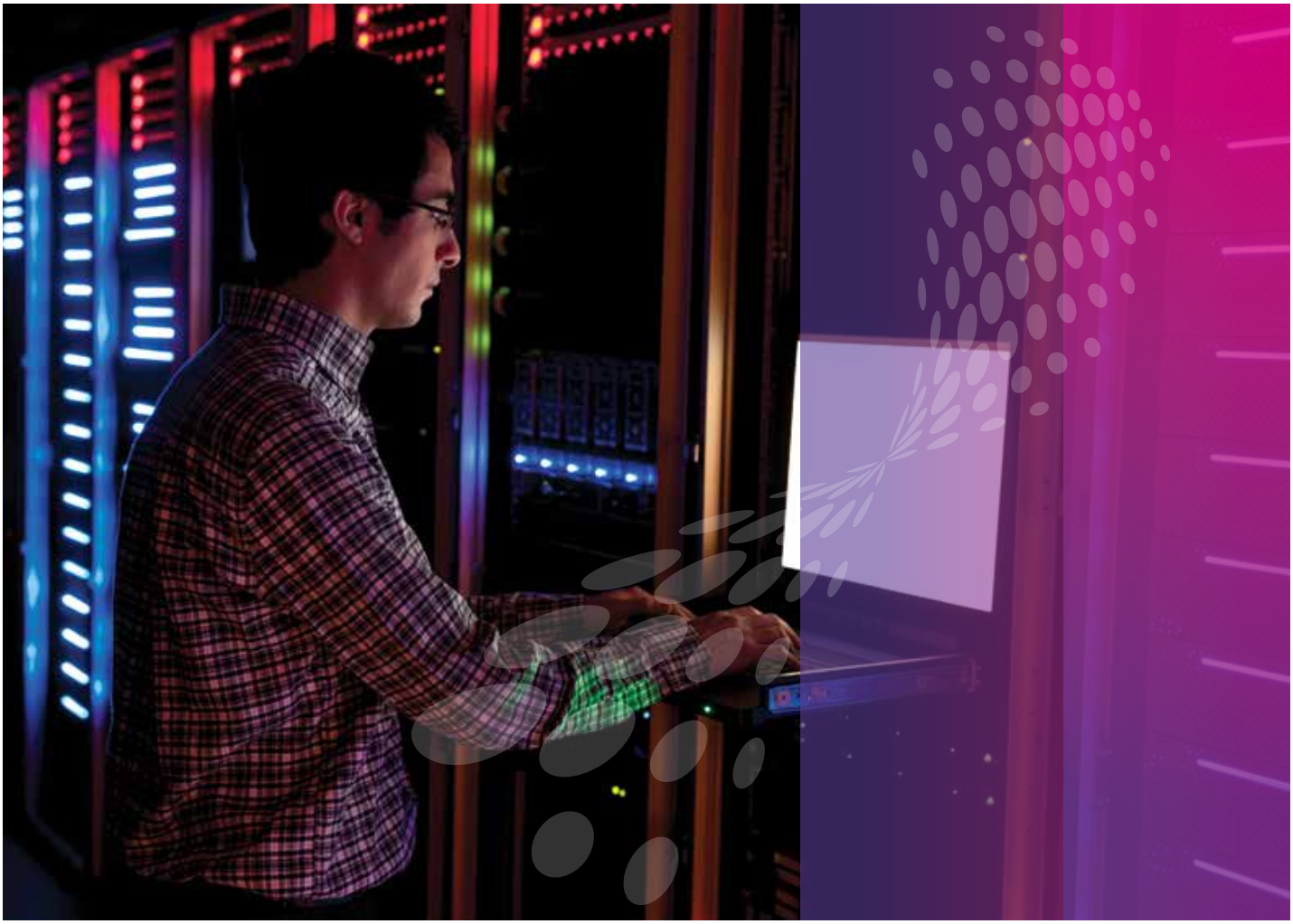
And the result is that today cybercrime almost exclusively leverages the lack of security-focused design in everything from your smartphone and web browser through to your credit card and even the electronic systems in your car.

The nature of threats

Cybercrime comes in a variety of forms ranging from denial of service attacks on websites through to theft, blackmail, extortion, manipulation, and destruction. The tools are many and varied, and can include malware, ransomware, spyware, social engineering, and even alterations to physical devices (for example, ATM skimmers).

It's no surprise then that the sheer scope of possible attacks is vast, a problem compounded by what's known as the **attack surface**: the size of the vulnerability presented by hardware and software. That is, if a hacking exploit works on Apple iPhones for example, and everyone in your organisation has one, then by definition the attack surface could range in the dozens to the thousands depending on the size of your company. Or, looking at it another way, if anyone with an iPhone is vulnerable, the attack surface worldwide totals in the hundreds of millions.

This is further compounded by the fact that hardware and software may provide multiple vectors for attacks, such that – and using the above example again – an iPhone might have multiple different vulnerabilities, each of them a possibility for exploitation. In some cases, multiple exploits can be used in tandem to hack a device, as the FBI recently demonstrated when it gained access to the San Bernardino shooter's iPhone (yes, the good guys can hack you, too...)



There were 19 distributed denial-of-service (DDoS) attacks that exceeded 100 Gbps during the first three months of the year, almost four times more than in the previous quarter. In some cases attackers don't even have to deliver on their threats. Researchers from CloudFlare reported that an extortion group earned $100,000 without ever launching a single DDoS attack.

Lucien Constantin,
Network World, 2016[28]

And this is to say nothing of embedded systems the type that of which power our infrastructure including transport, electricity, and communications. Here, attacks are often more targeted – even down to specific to systems in a particular plant – but the repercussions are also considerably more dangerous. Shutting down an electrical grid, for example, can have life-threatening consequences.

What you also don't see – because it's hidden in the millions of fibre-optic networks and routers that form the internet – is that attacks are happening constantly all around the world, even as you read this. Your modem at home that gives you access to the internet is constantly fending off queries to see if your IP address has any open ports (the virtual addresses that allow software to communicate to and from your computers and network).

According to network security and services company Fortinet, 500,000 attacks occur against its networks every minute[5]. And that's just one service provider.

The bottom line is this: almost anything controllable by technology will have a weak spot. In the past year we've seen everything from cars ("Hackers remotely kill jeep on highway"[6]) to medical devices ("Hackers can send fatal dose to drug pumps"[7]) to toys ("Hackers hijack Hello Barbie Wi-Fi to spy on children"[8]) succumb to anyone with a little knowledge, time, and opportunity.

To appreciate the scope of the challenge that lies ahead – the new types of threats that we are starting to see emerge now – and thus the importance of cybersecurity for the government, industry, and the individual, the following section delves into our predictions of where cybercrime is heading, and the type of attacks we can expect to see.

The Internet of Things (IoT)

For $6 in Bitcoin, I can rent time on a DDoS tool and bring down most websites. Better yet, if I send just the right type of packet to their web servers, I can crash the site for free.

A Thief's Perspective (interview), Intel Security, 2015[18]

Perhaps the most recognised buzzword of the moment, the Internet of Things (IoT) encompasses the many and varied devices currently on the market, or soon to be on the market, that will connect to and stay connected to the internet 24/7.

Typically this includes products like webcams, smart TVs, and even the much touted internet-connected fridges. But IoT actually encompasses a broad range of products most of which you won't actually see – electronics, sensors, actuators and software soon to be built into everything from your car to your home: technology to unlock your door and turn on the lights when you arrive home; technology to allow cars to talk to other cars and traffic lights to prevent accidents; technology to let entire cities regulate air-quality, manage energy distribution, and regulate water supply all in real-time from thousands of buildings, each with thousands of sensors, all communicating through a city-wide network.

Sound like fantasy? There is already a development in the UK by River Clyde Homes and the Hypercat Consortium to build a Smart Neighbourhood in Scotland by installing hundreds of IoT devices to monitor everything from temperature and local weather through to carbon monoxide levels, potential gas leaks, lift maintenance, smoke detection and communal lighting to name a few. All of these talk to each other to provide an overall real-time knowledge base for the operating of neighbourhood services, and to minimise health and safety risks.

But this is just the beginning. IoT has the potential to encompass a lot more – heart monitoring implants, pathogen monitoring for food, transponders for animals on farms, environmental waste monitoring, field devices for police to detect threats, feedback sensors for firefighters in search and rescue and much, much more.

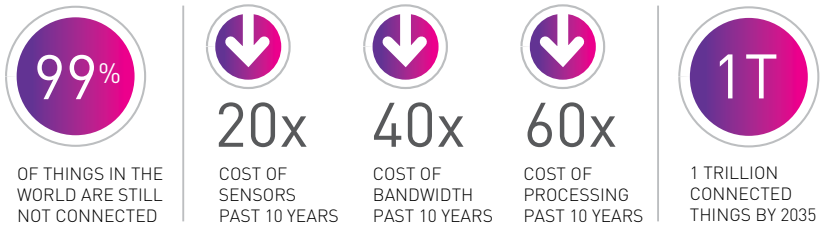
Perhaps the best way to imagine IoT is – and to borrow a phrase from a research paper at the Social Science Research Network – is to think of IoT as an "inextricable mixture of hardware, software, data and service"[11]. Which of course is to say that the potential is close to limitless.

According to the CEO of Cisco, Chuck Robbins, the IoT industry is expected to be worth $US19 trillion globally by 2020[12]. Closer to home, Frost & Sullivan is tipping the Australian market for IoT – just in terms of home devices, such as in security or energy management – to be worth $200M by 2020.[13]

Taken together, this means is that in the near future just about everything you use, and everywhere you go, devices will be hooked up to each other communicating, sharing data, and enabling a future that once was the realm of science-fiction. The potential boon for society is immense, but so too are the risks.

IOT – A FUTURE OF CONNECTED DEVICES

As barriers to entry drop we will see an uptake of IoT, creating a future where attack vectors are everywhere.
Source: IoT Alliance Australia



Considerably more devices will be connected to each other and the internet: Intel predicts there will be as many as 200 billion devices by 2020.[14]

And if you remember our primer at the start of this document, that is one very large, very vulnerable attack surface. It should go without saying that the threat potential from IoT is beyond vast, and therefore cybersecurity practices must form part of IoT development from the ground up. For example, car manufacturers need to build security protocols into the sensors in smart cars to ensure they can't be turned against the driver to cause injury or death. Something which, unfortunately, is currently not the case (see next section, **Autonomous systems**).

Although a successful attack on industrial IoT devices with an installed base of hundreds of millions would likely cause havoc, one device at a key point in a critical infrastructure control system could be far more devastating.

McAfee Labs 2016 Threats Predictions[15]

Botnet armies

Somewhat related are botnets. A bot (sometimes called a 'zombie') is a remotely-controlled and compromised – unbeknownst to the owner – computing device that's connected to the internet. This could be a desktop computer or a laptop, but it can also be a webcam, a modem, or a Wi-Fi router, all of which almost everyone has in their home today. Unfortunately, again, poor security design sees devices like these come with only basic security that can be easily bypassed, allowing cybercriminals to install malware and control the device remotely.

Collect enough bots and you have a botnet, and with a botnet you can launch a distributed denial-of-service (DDoS) attack. In large enough numbers, such an attack can take down websites and knock services offline – something we saw first-hand earlier this year when the Australian Bureau of Statistics eCensus website was very publicly attacked.

This is to say nothing of what happens when IoT devices take part in a DDoS, which we know they already do. In fact, the world's largest DDoS occurred in August of this year knocking out French internet service provider OVH, suffering an attack that transmitted a record-breaking 1Tbps[17]. To put this into perspective, a 1Gbps attack is sufficient to knock most businesses anywhere in the world offline, and this attack was 1000 times stronger. It was only earlier in 2016 that the previous record came in at 579GBps. That is, we have already seen almost a doubling of capability in less than a year, and at a volume so high that very few very large players – the Googles and Akamais of this world – are able to withstand.

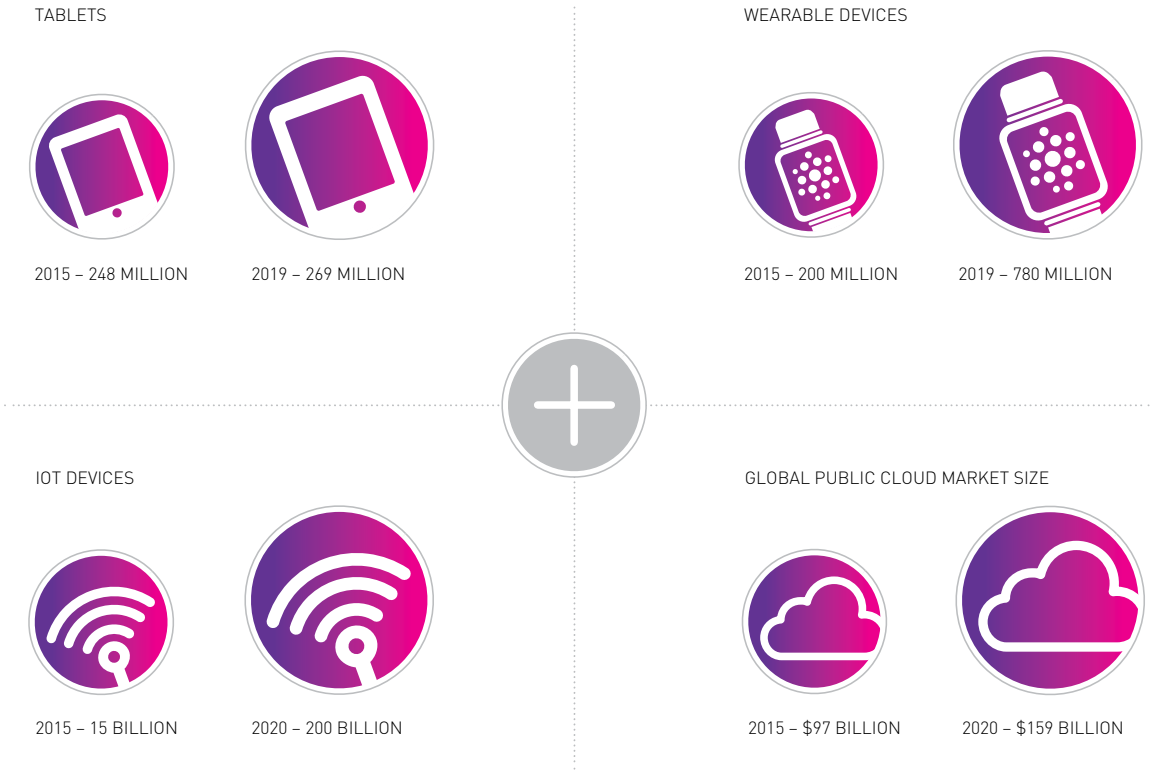
Analysis of the attack on OVH revealed it consisted of some 145,000 devices, the majority of which belonged to internet-connected CCTV cameras and DVRs (digital video recorders) typically used in business and home surveillance.

Such products make ideal bots because their limited functionality provides less scope for security software; they're often headless, meaning a user doesn't have a display or other means to interact with them to monitor activity. They almost always come with a default administrator password that nobody changes because it requires effort and a bit of technical know-how – allowing cybercriminals to walk through the front door and take it over.

This is a great example of how lack of security design enables cybercrime – who would think to hack a CCTV? But that's the line of thinking that engenders security flaws. And once a flaw is out there, it often can't be fixed: the cost of updating the devices could be ruinous for a company if they need to be recalled, as not every device supports the ability to be updated remotely.

Prevention, then, is better than cure.

Recently, cybercriminal botnet operators have moved to self-sustaining botnets that continually find new devices to infect and add to the flock, even while others may be taken offline[16]. This has led to cybercriminals to sub-lease access to their botnets on the cheap, meaning anyone with a grudge and $50 can bring down a website.



MORE DEVICES, MORE THREATS

The growth in user-centric mobile and IoT devices will see greater exploitation of personal data.
Source: McAfee 2016 Threats Predictions

WHEN SECURITY IS AN AFTERTHOUGHT

One of the most potent botnets to date is **Lizardstresser**, by the infamous Lizard Squad DDoS group. In 2015 the group released the source code, allowing others to make their own. This has resulted in copy-cat groups and a stark increase in botnets-for-hire.

Lizardstresser relies on cheap IoT hardware to build large botnet armies, using shell scripts (simple text-based scripted programs) to scan IP ranges and to attempt access using hardcoded usernames and passwords (usually all related to administrator logins).

It's so successful because many IoT devices are manufactured with the same default login credentials. Additionally, these same devices are also often simply plugged in and turned on, and have unfettered access to the internet through whatever corporate or home networks they are connected to. This makes them easy targets to enslave into botnets.[19]

Attacks on automobile systems will increase rapidly in 2016 due to the rapid increase in connected automobile hardware built without foundational security principles.

McAfee Labs 2016 Threats Predictions[15]

Autonomous systems

As technology continues to permeate our lives, we move from operating technology to integrating with it. This is especially true of autonomous systems that are by definition designed to blend in with our society, becoming second nature.

By the same token however, reliance on such systems makes the outcome of their abuse potentially more damaging. Typically, these technologies also integrate into critical infrastructure, such as payment systems and – in the case of autonomous cars – the transport network, making protecting them from a cybercrime a pivotal focus for cybersecurity.

Driverless cars and transport

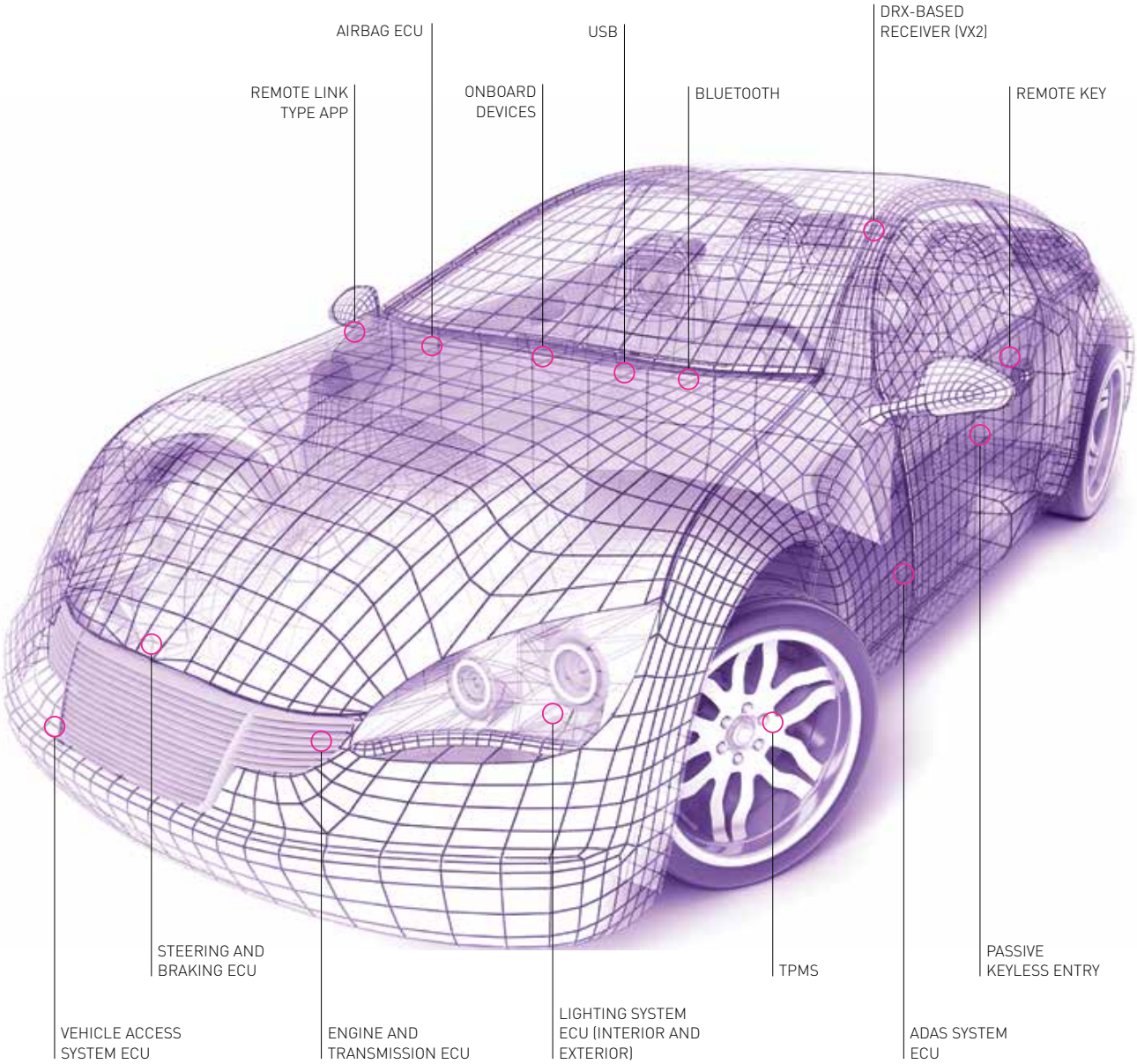
At the moment, driverless cars are stealing the limelight of autonomous systems. While so far there have been no documented cases of wilful misuse, it's already been demonstrated that autonomous cars can be remotely controlled.

In 2015, 1.4 million Jeep Cherokees were recalled after hackers demonstrated that the cars could be taken over remotely through the entertainment system.[6]

Similar abuse of access has also been demonstrated with cars from Mercedes, BMW, Toyota, Audi and Fiat – all due to poor security in the design process.[20 21 22]

It's not hard to see that in the wrong hands such abuse could result in cars being used as weapons to maim or kill pedestrians – or even the occupants themselves – on the road. According to Business Insider in its Connected-Car Report, there will be 220 million autonomous cars on the road by 2020.[23]

McAfee's 2016 Threats Predictions Report notes that "poorly secured driverless cars and smart highways will further expose drivers and passengers in 2017 and beyond, likely resulting in lost lives...", and that "recent vehicle hacks are a great example... selectively modifying communications and commands so they can take control or affect what the vehicle does. This has a potentially terrifying result."[15]



THE ATTACK SURFACE OF A MODERN CAR

Many car systems have not been designed with security in mind, making it possible to hack into a car via smartphone or laptop.
Source: McAfee 2016 Threats Predictions

BIRTH AND REBIRTH OF A DATA BREACH

An example of how one breach can lead to another (in this case, harvesting payment data of consumers after first breaching a POS vendor).
Source: Verizon 2016 Data Breach Investigations Report

They'd been inside our network for a long period, about two years. And the way it was described to us was they're so deep inside our network it's like we had someone sitting over our shoulder for anything we did.

Daryl Peter, IT Manager, NewSat 2012-2014[85]

ATMs and Point of Sale

Credit cards have long been the target of fraudsters, spurring the development of RFID chips and other protective technology in the banking ecosystem. However, security is an arms race and threats such as skimming is now a global phenomenon that allows data from cards to be read and transmitted wirelessly in real time from ATM machines and point of sale devices.

Indeed, point of sale systems as a whole are their own a sub-category of cybercrime infiltration, being the weakest point of the payment processing system, and so it's not uncommon to find malware specifically designed to pull data from embedded systems in POS terminals (see 'Birth and re-birth of a data breach' diagram, above.)

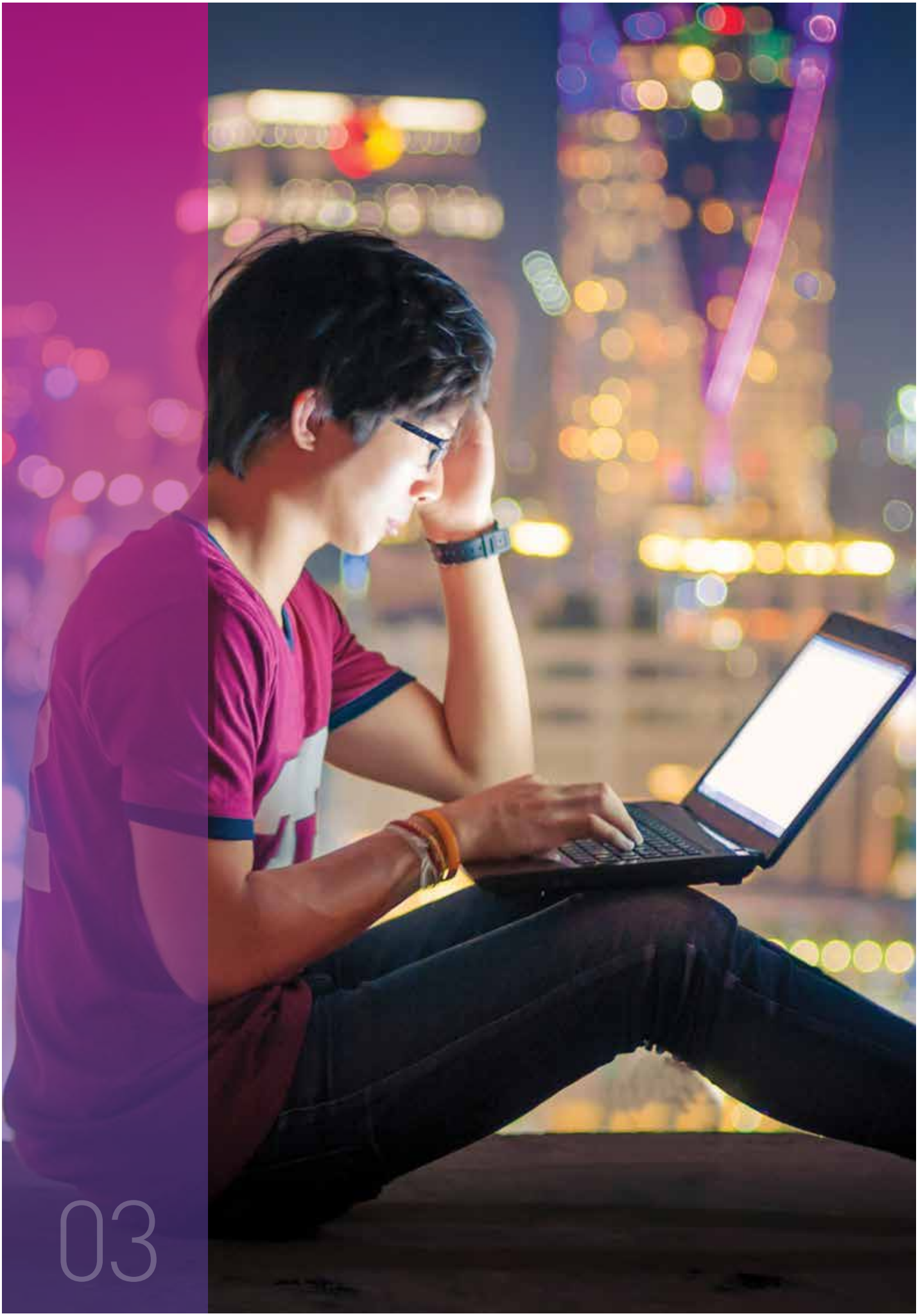
Now, of course, the technology has progressed further with contactless pay systems from the likes of Apple (Apple Pay) and Google (Android Pay), as well as players like Samsung (Samsung Pay, of course) that allow consumers to pay simply by waving their smartphone over a device – which presents yet another attack surface for cybercrime.

WHAT ABOUT WEARABLES?

Wearables are rapidly gaining popularity with smartwatches such as the Apple Watch and Samsung Gear, as well as exercise wearables like those from FitBit and Jawbone. According to ABI Research, an estimated 780 million wearable devices will be in circulation by 2019.

Now you might be wondering just what would be so bad about hacking a fitness wearable? This is exactly the line of thinking that allows cybercrime to occur.

Wearables are tracking all sorts of personal information including GPS location, blood pressure, heart rate, and anything else you feed them such as weight or diet. Such personally identifiable information could be used as a base to target you for spear-phishing, or aid in identity theft. But the real opportunity is these devices linking to your smartphone, where phone numbers, more personally identifiable information, emails, web logins etc. could theoretically be compromised.



03

Cyberwarfare

Most modern countries now are treating cyberspace as another military domain, in addition to land, air and sea.

Dmitri Alperovitch, Cybersecurity industry executive[25]

Once the domain of science fiction, cyberwarfare is now very real, with most superpowers now having dedicated cyberwarfare divisions of the military. And while there have been few known, co-ordinated cyberattacks on physical targets, we don't need a crystal ball to predict the future: they will only increase.

It's telling that we are now in an age where governments, political groups, criminals and corporations can engage in cyberespionage, cyberwarfare, and cyberterrorism. The Prime Minister, Malcolm Turnbull, announced at the Australia-US Cyber Security Dialogue in September that Australia is well equipped to both defend against and carry out cyber-operations.

We now live in a world where warfare can be conducted entirely virtually – though the consequences will almost always have repercussions in the physical world.

Automated attacks

Much of what we talk about with regards to 'hacking' is a function of people at keyboards finding and abusing weak links in security. It is a skilled and time-consuming process.

However, in the ever-evolving arms race between subversive elements and cybersecurity, a move to automating such attacks would have clear benefits: whereas exfiltration may have taken days by skilled personnel, automated attacks can reduce this to hours – infiltrating, searching for a payload, gobbling it

ENERGETIC BEAR

One of the more well-known nation-state sponsored tools of cyberwarfare currently active is Energetic Bear. First uncovered in 2012, and believed to be sponsored by Russia, Energetic Bear used the Havex Trojan to gain access to company networks, particularly those in the energy sector, though it has also been found in manufacturing, construction, health care and defence companies.

Primarily designed for cyberespionage, when the threat was first mapped in 2014 by security firm Kaspersky Labs, it identified nearly 2,800 victims worldwide, affecting countries including the US, Spain, Japan and Germany.[44]

Almost half the security professionals surveyed think it is likely or extremely likely that a successful cyberattack will take down critical infrastructure and cause loss of human life within the next three years.

Critical Infrastructure Readiness Report, Aspen Institute and Intel Security, 2015[25]

up, encrypting it, and sending it out over the network before the host machine's security personnel even knows what's happened.

The defence to which, of course, is to automate security to combat automated attacks – computer software fighting computer software, all without human intervention. And while this sounds like a sci-fi movie, the reality is it's already here – in August this year the world's first automated cyber-hacking contest was held at DARPA (Defence Advanced Research Projects Agency), which saw supercomputers battle it out for a $2 million prize, the win going to a perhaps appropriately named machine called 'Mayhem'.[45]

30,000

PEOPLE LOST POWER WHEN 30 SUB-STATIONS IN WESTERN UKRAINE WERE SHUT DOWN VIA A REMOTE ATTACK

Cyberattacks on infrastructure

As societies around the world depend ever more heavily on technology, the ability to shut down or destroy infrastructure, take control of machines and vehicles, and directly cause the loss of life has become a reality. To date, some of the more well-known examples of cyberattacks on infrastructure include:

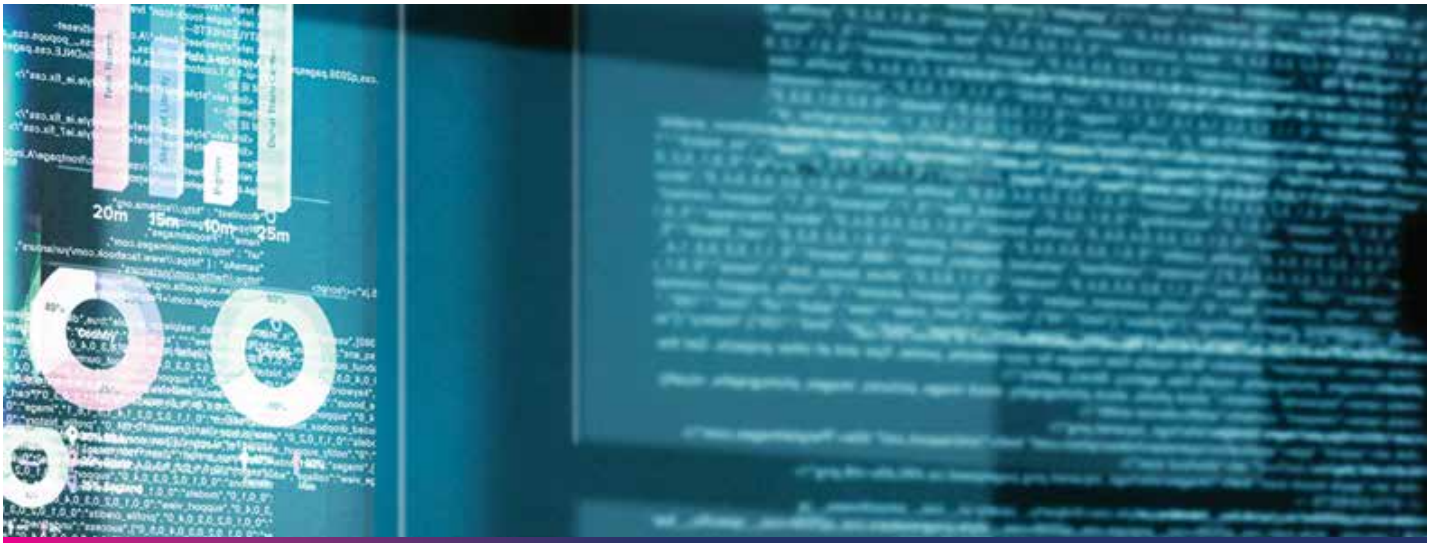
- In 2008 when Russia sent tanks into Georgia, the attack coincided with a cyberattack on Georgian government computing infrastructure. This is thought to be one of the first land and cyber coordinated attacks.[39]
- Also in 2008, Stuxnet – a computer worm purportedly jointly designed by the US and Israel – crippled Iran's nuclear-enrichment program by sabotaging centrifuges.[40]
- In 2014 a German steelworks was disabled and a furnace severely damaged when hackers infiltrated its networks and prevented the furnace from shutting down.[41]
- In 2015, with an attack strongly suspected to have originated from Russia, 230,000 people lost power when 30 sub-stations in Western Ukraine were shut down via a remote attack. Operators at the Prykarpattyaoblenergo control centre were even locked out of their systems during the attack and could only watch it unfold.[42]

In all of these, and as an indication of how the landscape of war is changing, the weapon of choice for these attacks wasn't guns or bombs – it was a keyboard.

French Coldwell, Chief Evangelist at governance, risk, and compliance apps company Metricstream, at a cybersecurity summit earlier this year noted that "this is the canary in the coalmine. Much more of this will come."[43]

We can expect governments around the world to strengthen their cyberattack and defence capabilities, spurring an arms race that will operate at a much faster pace than we saw in the Cold War. But here the results could be much more subtle – as noted in the McAfee 2016 Threats Predictions report, "they will improve their intelligence-gathering capabilities, they will grow their ability to surreptitiously manipulate markets, and they will continue to expand the definition of and rules of engagement for cyberwarfare."[15]

03



America's top spies say the attacks that worry them don't involve the theft of data, but the direct manipulation of it, changing perceptions of what is real and what is not.

Patrick Tucker, Defense One[27]

WHEN SOFTWARE KILLS

It's easy to forget that computers can have life-threatening consequences. Here are some well-known examples of what happens when technology fails due to small mistakes in computer code.

Therac 25

This is so well known that it's now taught in computer science curriculums. Therac 25 was a Canadian medical machine designed to help save lives by administering targeted doses of radiation to kill cancer. Instead, a rare software glitch saw patients receiving 100 times the necessary dose. In a period from 1985-1987 five patients died, while many others were seriously injured.[29]

Patriot missile

During the Gulf War in 1991 a Patriot missile failed to intercept a Scud missile due to a software fault, resulting in the death of 28 US soldiers and injuring 100 others.[30]

Toyota's ETCS

Toyota recalled 8 million vehicles worldwide starting in 2009 after faults with the Electronic Throttle Control System resulted in the death of 89 people.[31]

Tesla's autopilot

In July 2016 a man died while relying on the autopilot function of his Tesla Model S when it failed to detect a trailer, crashing into it.[32]

These are examples of unintended software faults, but subtle manipulation of data could intentionally result in loss of life, and remain undetected until this occurs. Military officials in the US have even raised concerns that Chinese hackers known to have infiltrated defence contractors over the last decade could have already altered code for weapon systems, sitting dormant until the next major conflict.[33]

Data manipulation

The biggest threats in cybersecurity today are around the large scale proliferation of targeted attacks – from breach and email distribution of socially engineered ransomware to potentially harmful attacks on critical infrastructure like energy networks.

Rodney Gedda,
Senior Analyst, Telsyte[53]

Not all attacks are about theft or destruction. A more sinister cause is the manipulation of data in place – such that machines can be controlled – or the wrong information reported to human operators without their knowledge.

It's clear if a cybercriminal releases stolen usernames and passwords on the web. It's much less clear if data belonging to a business has been modified – with those who own the data none the wiser. As no destruction is caused such intrusions here can be harder to detect, if they're detected at all. Yet even the smallest alterations can have serious consequences and implications.

James Clapper, Director of US National Intelligence, said it succinctly when he stated, "Decision making by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving."[27]

Backdoors and espionage

Backdoors are particularly concerning because they can be both hard to discover and provide unfettered access to a system or entire network.

A compromised system can provide cybercriminals or a nation-state the ability to spy on data, or alter the data in place. And for as long as a system is compromised, abuse of privilege will be ongoing.

By way of example, in 2015 Juniper Networks announced it had discovered multiple backdoors in its firewall operating system code installed with its products – the same products used to protect corporate and government systems around the world. These backdoors had been active for at least three years.

One of the backdoors gave remote control of the firewall to an outside user, while another disturbingly allowed for the decryption of traffic running through a Juniper Networks firewall, allowing traffic to be eavesdropped. The sophistication and nature of this breach points to a nation-state as the culprit.[34]

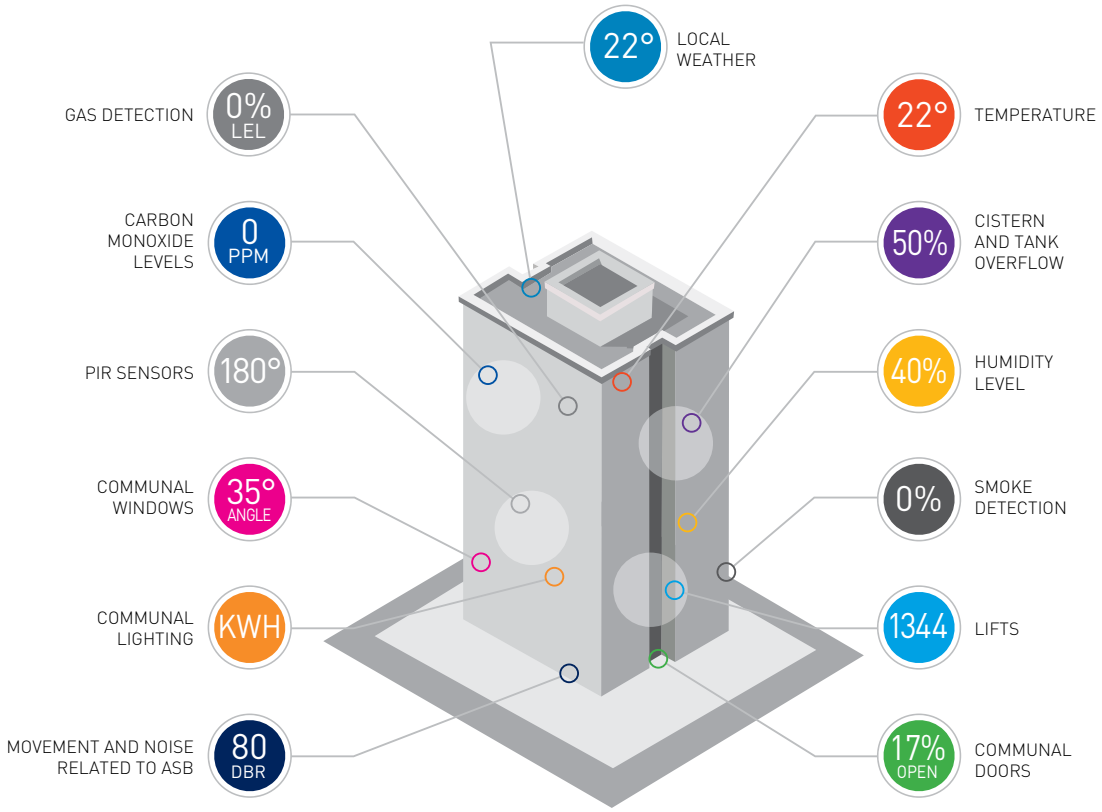
Cloud concerns

As with any successful technology, the more popular it becomes the larger a target it also becomes. Cloud is now well entrenched as a concept and a service offering, and indeed many businesses now rely on cloud services to operate.

On the one hand this can make security easier for companies outsourcing their data to lie on a cloud service where the cost of security is carried by the vendor, but on the other it centralises cloud services as highly viable targets for attack.

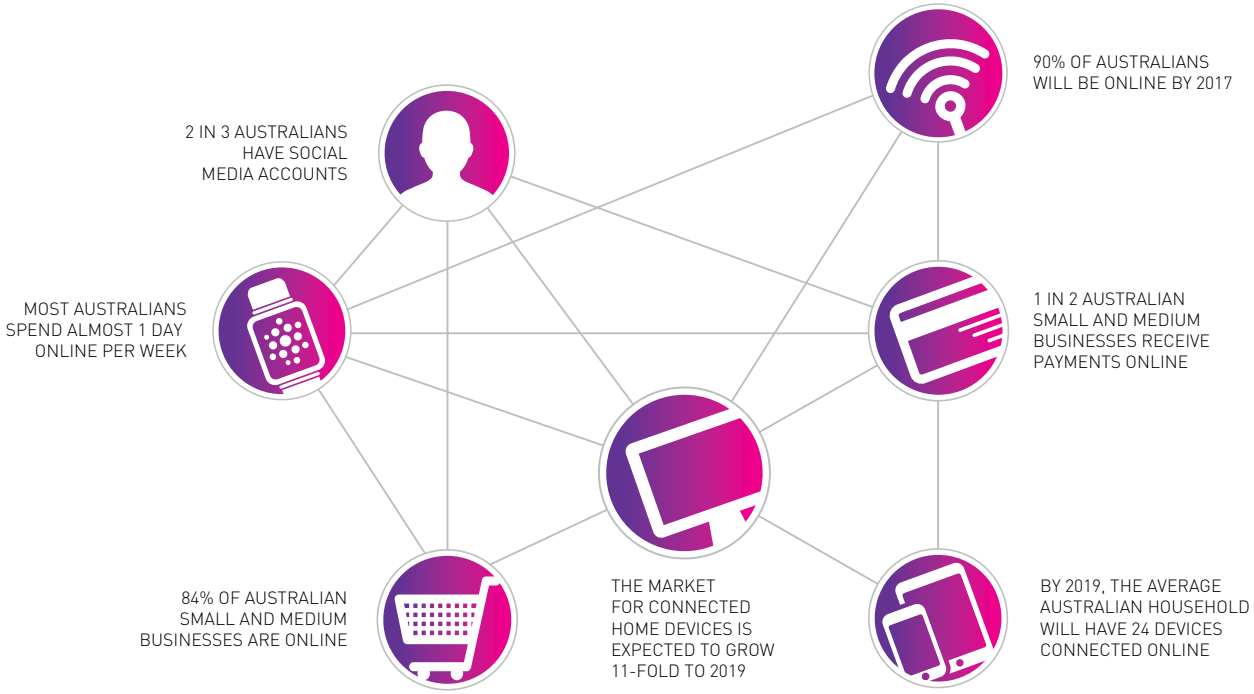
BLAST FROM THE PAST

Perhaps one of the more prominent examples of cyberwarfare – even before the internet became ubiquitous – comes from the cold war in 1982 when a Siberian oil pipeline exploded, creating at the time one of the largest non-nuclear explosions in history, so large it was visible from space. Later the cause was revealed to be a Trojan horse implanted by the US in pipeline equipment sold from a Canadian company on to Russia. End result: economic sabotage facilitated by computer software.



SMART CITIES – BRITAIN'S NEIGHBOURHOOD@BROOMHILL PROJECT

A small sample of the types of IoT sensors in a smart city apartment block.
Source: IoT Alliance Australia



AUSTRALIANS ARE BECOMING INCREASINGLY CONNECTED ONLINE

As Australia becomes ever more connected, cybersecurity becomes ever more important. Source: Commonwealth of Australia, Department of the Prime Minister and Cabinet, Australia's Cyber Security Strategy.

Nation-state cyberwarfare will become an equaliser, shifting the balance of power in many international relationships just as nuclear weapons did starting in the 1950s.

McAfee Labs 2016 Threats Predictions[15]

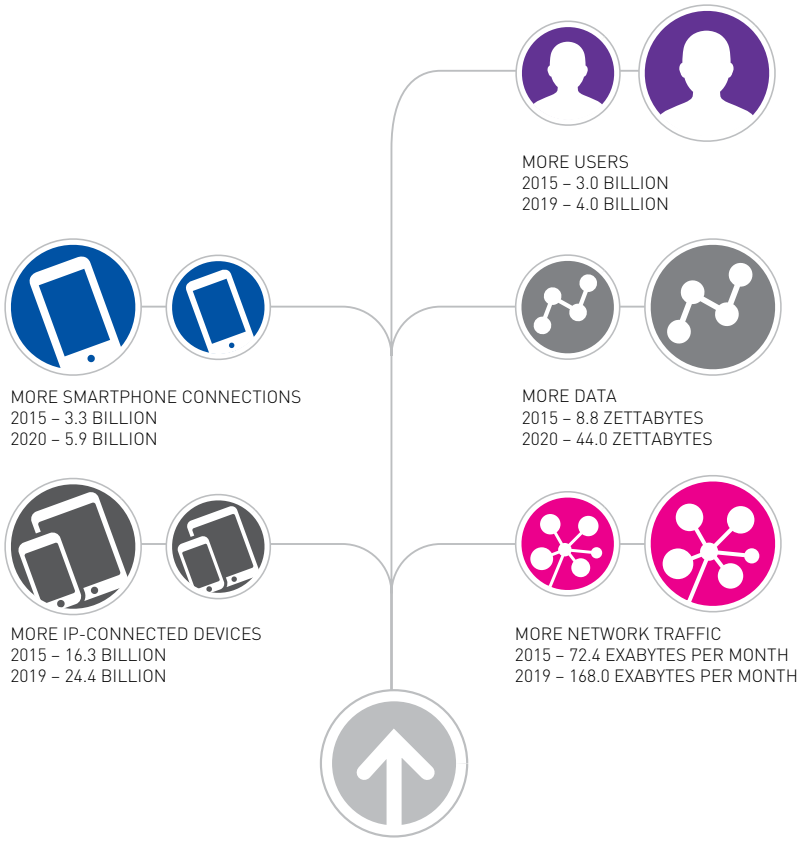
But there's also a less obvious concern here: sovereignty.

Security of cloud data is not just about encryption, but also the sovereignty of access when data is physically located in an overseas jurisdiction. The internet may have no borders, but data itself still lies within traditional real-world boundaries and in turn may be bound by the laws of a foreign nation.[35]

Further, even if we trust in the laws of a foreign nation there's no guarantee they won't change, and data that was previously protected could be subpoenaed, accessed by government departments, or shared with third parties without consent.

A good example of how the landscape can change is the news earlier this year that in Russia, ISPs are now required to store both the metadata and content of communications, and hand over encryption keys for any encrypted data[36]. Any cloud data passing through an ISP can become readable by Russia's government and intelligence services. This had the immediate fallout of some popular VPNs closing their Russian nodes, and in at least one known case[37] servers were seized from the VPN provider under this law.

With cloud expected to grow by around 18% through 2016[38], concerns around the sanctity and sovereignty of cloud data are only going to increase.



THE GROWING CYBERATTACK SURFACE

More devices, more users, more data – every year.
Source: McAfee 2016 Threats Predictions

Virtualised threats

As a result of the growth in cloud services, there has been an explosion in the use of virtual machines for business, making these prime targets for cybercrime.

Fortinet notes, "growing reliance on virtualisation and both private and hybrid clouds will make these kinds of attacks even more fruitful for cybercriminals."[5]

And, as the McAfee's 2016 Threats Predictions report notes, "how do you accurately track and attribute an attack, with all of the obfuscation possible with clouds and virtualisation?"[15] It goes on to state, "if we keep our stuff in the cloud and access it from a phone, tablet, kiosk, automobile, or watch (all of which run different operating systems and different applications), we have substantially broadened the attack surface."

Indeed, the use of apps that rely on the cloud will also allow mobile devices running compromised apps as a way for hackers to remotely attack and breach public and private corporate networks.[5]

Finally, there's one other consideration: cybercriminals can use cloud services themselves, providing powerful resources for processing power and storage, and the ability to appear and disappear at the click of a button.

Industry and the individual

Malware is still very popular and growing, but the past year has marked the beginnings of a significant shift toward new threats that are more difficult to detect, including file-less attacks, exploits of remote shell and remote control protocols, encrypted infiltrations, and credential theft.

McAfee Labs 2016 Threats Predictions[15]

While large security breaches make the news, the majority of cybercrime involves fraud targeting businesses and individuals. Here, a mixture of malware and social engineering can see financial fraud resulting in the loss of thousands, all the way up to millions, of dollars.

And, it's also some of the hardest crime to combat – largely due to the sheer scope of attack surfaces which can range from desktop computers through to laptops, tablets and smartphones.

Sometimes, the vector is simply a phone: using social engineering through an employee to gain access to a network, or con an individual out of money – as in the classic **technical support scam**, of which the Government has a great summary at www.scamwatch.gov.au (also a great site to learn about other online scams).

Ransomware and Cryptoware

The ease with which amateur cybercriminals can get their hands on tools to extort money is increasing. So far in 2016 we've seen a prevalence of cryptoware targeting both enterprise and individuals, requiring the payment of a ransom to unlock encrypted files.

The most well-known of these was Cryptolocker, said to have earned its creators $US3 million before it was shut down by a consortium involving the US, the UK, and a number of security vendors and researchers.

While in an ideal world these ransoms would never be paid – and thus not encourage extortion as a business model – with victims opting to restore data from backups instead, the reality is that this isn't always practical. This is especially true for companies, where the downtime or lost productivity from denied access to the data can be higher than the price of the ransom.

Recently, however, the ante was upped with the appearance of ransomware that claims to have encrypted files and asks for payment for the decryption key, but in fact the files have simply been deleted unbeknownst to the owner.[46] Known as **Ranscam**, the one upside to this change in tactics is that if it becomes the prevalent form of ransomware, it will destroy the trust – or what little there is – between the criminal and the victim that the data will be recoverable. No honour among thieves, it seems.

Multi-vector attacks

Taking advantage of multiple concurrent attack mechanisms, a single attacker may try to penetrate an organisation on multiple levels in order to access different data, such as targeting the CFO with social engineering, with the aim to secure financial information while using spear-phishing targeted at office staff to get malware installed.

Utilising the cumulative bandwidth available to these IOT devices, one group of threat actors has been able to launch attacks as large as 400Gbps.

Arbor Networks on LizardStresser[19]

THE WORLD WE LIVE IN

Facebook CEO, Mark Zuckerberg, has been observed in a promotional photo for Instagram with his laptop in the background sporting tape covering both the camera and the microphone – the implication being he doesn't trust his own machine is secure from cyberespionage.[24]

If the CEO of one of the world's technology innovators can't necessarily trust his own computer, what does that mean for the rest of us?

One of the largest known (considering not all companies like to own up to having been scammed) scams to date resulted in the loss of €40 million from Leoni AG[84] in August of this year, facilitated by tricking a financial officer into transferring funds to the wrong account.

Importantly, success with one method can lead to exploitation of others, such as an employee clicking on a macro within an email which in turn downloads a program, which then automatically pulls down targeted malware to access network resources (this is sometimes known as 'weaponised email attachments').

The Aspen Institute's Critical Infrastructure Readiness Report notes "the analysis of this year's data led to an interesting new revelation – nearly 70% of attack victims are targeted for the purpose of advancing a different attack against another victim. For instance, an attacker may hack a website to serve malware to visitors with the intentions of infecting its true target."[25]

A common adage in cybersecurity is that while defence must consider every possible attack vector, attackers only need to find one weak point. An attack only needs to be successful once.

Identity theft

Identity theft is the crime no one thinks will happen to them until it does.

According to Javelin Strategy and Research, some $US16 billion was stolen from 12.7 million consumers in the US alone during 2014 due to identity theft.[26]

However, identity theft is more than just financial fraud, it's a central pillar for all manner of cybercrimes: once you can impersonate an individual, you can gain access to their accounts, commit multiple types of fraud in their name, steal information only they have access to, and much more.

As we share more of our lives online, we open ourselves to being exploited further. In McAfee's 2016 Threats Predictions report the authors note that "the growing value of personal data… is already more valuable than payment card information and will continue to climb."[15]

The future in our hands

Asia-Pacific is rapidly emerging as a potential market for cybersecurity solution providers, driven by emerging economies such as China, India and South-East Asian countries.

Cybersecurity Ventures[48]

$639 Billion

ESTIMATED WORTH OF THE CYBERSECURITY INDUSTRY BY 2023

It should be clear by now that we live in a world reliant on technology, and that this technology can also be vulnerable if it's not designed with security in mind. While some products and services are, many more are not, and to this end the development of cybersecurity tools, skills, and education is essential to protecting both our infrastructure and way of life.

Globally, the industry is worth $US106 billion with estimates projecting its value at $US639 billion by 2023[1]. As a nascent industry, there is a real opportunity for Australia to become a centre of cybersecurity excellence with the right leadership and investment.

Additionally, as cybersecurity must underpin the design of almost any technology product that comes to market, it goes without saying that if we don't develop our own cybersecurity products and services then we need to purchase them from overseas.

However, there is real value in producing cybersecurity products and services locally, not the least of which is control over the source code – ultimately, you must trust an overseas vendor that there are no backdoors or mechanisms in their software and firmware that would allow either exploitation by a foreign nation's government departments (such as intelligence agencies), or exploitation by cybercriminals discovering these vulnerabilities.

Particularly when it comes to national cyber defence, it would be preferable to utilise home-grown products. Not doing so is, in the words of Alex Scundurra, CEO of fintech hub Stone & Chalk, "like outsourcing our defence force to someone else."[56]

Achieving any kind of growth for a local cybersecurity industry will require support of the government, private sector, and academia. We know that as we depend more and more on technology the demand for qualified cybersecurity specialists, products, and services is only going to increase – so it's in our best interests to work towards developing and harnessing our own cybersecurity sector.

THE 100% SECURE COMPUTER

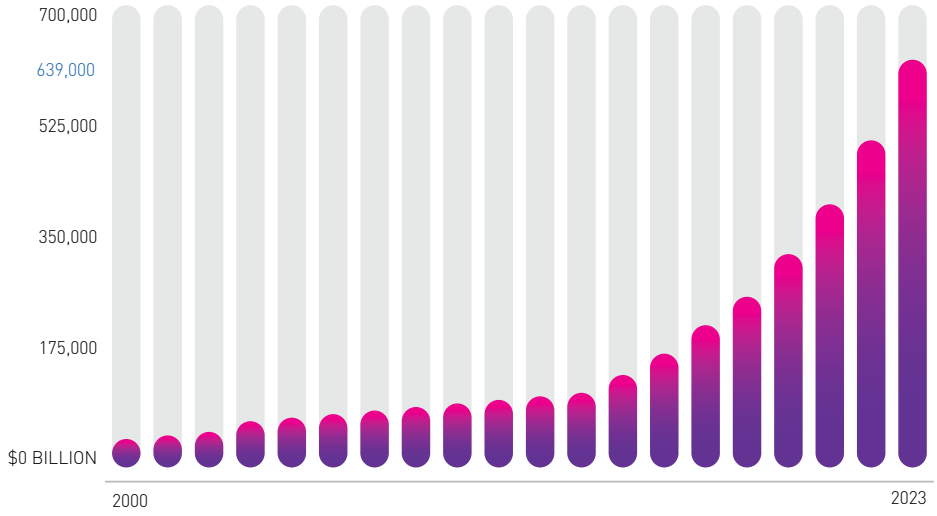
When it comes to security you can never completely eliminate risk, you can only minimise and mitigate it – there is no such thing as the 100% secure system.

The adage goes that the only **truly** secure computer is locked in a lead box, buried fifty feet underground, sealed with concrete, with no wired or wireless connections in or out.

And turned off.

Which is to say, not a very useful computer.

Ultimately, for the majority of cases, security is about making the cost of entry higher than the value of the assets being protected.



ESTIMATED GLOBAL CYBERSECURITY SPENDING TO 2023

An estimated ten-fold increase in spending as cybercrime becomes a pivotal focus.
Source: IT-Harvest

Opportunities

Cyberattacks are costing global businesses as much as $500 billion per year... The banking and financial sectors have led the way as top targets for cyberattacks in the last five years, with IT and telecom, defence, and the oil and gas sectors following behind.

Cybersecurity Ventures[48]

The threats are many and varied, but so are the opportunities – technology constantly teases us with new ideas, new products, and new ways of living our lives. It also presents new economic opportunities, new ways of doing business, and new ways to make a difference.

The data-driven economy

If there's one prediction we can make about the next decade it is this: data will be king. From machine-learning AI to the Internet of Things, the accumulation and analysis of data from every aspect of our lives will drive entirely new insights and products.

We already have advanced local information system industries to support this, including the emerging FinTech sector (where already nine Australian FinTech businesses are listed in the world's top 100 FinTech companies[47]).

But the opportunities for products and services involving data are going to increase exponentially – already we are creating new ways to mine data and produce new services (right down to robot lawyers[86]). Combined with the Internet of Things, there is tremendous economic opportunity for Australian technology companies to innovate and produce products for the world stage.

But all of these will also require cybersecurity as a fundamental building block. Regardless of the level of investment or development in Australian technology businesses, we will need a vibrant cybersecurity sector to support innovation and guarantee the economic prosperity of technology initiatives.

Security is as much about software as it is about awareness. It takes sophisticated coding to develop ransomware, but only one click to activate it.

Rodney Gedda,
Senior Analyst, Telsyte[53]

Technology as wealth creation

The benefits of technology have created tremendous wealth over the last decade – you only need to look at household names like Google, Apple, or Facebook for examples.

As we move to a world populated by internet-connected devices – from your car to your fridge, your children's toys and even the clothes you wear – there are still Googles and Apples and Facebooks to be discovered.

This alone represents tremendous opportunities for Australia's ICT sector, but for any of this to be possible, the gadgets and the networks they communicate on must be secure, and this means cybersecurity will need to form the basis of every new technology going forward.

The end result, as it happens, is that good cybersecurity is good for the bottom line. There is an inherent interest for companies to implement good cybersecurity strategies to ensure their profitability is protected, and this in turn will require cybersecurity products and skilled cybersecurity professionals in the workforce.

The economic opportunity for Australia then for a strong cybersecurity sector is clear.

Cybersecurity as job growth

According to SEEK, cybersecurity roles are already in demand, having grown 57% in the last year.[50] This includes jobs like Security Analyst, Security Architect, Security Engineer, and Chief Information Security Officer, all of which represent the new type of opportunities that are developing in the workforce.

We have the skills and talent in Australia to support and capitalise on this growth, which will only see more demand as the importance of cybersecurity in the development of new technologies and products continues to grow.

There are lessons to be learned from Israel's high proportion of security vendors here: moving from a high proportion of agricultural exports some 50 years ago, one of Israel's primary exports is now software. Government support for a startup culture and the belief that technology is the backbone of a strong economy has seen Israel now lead the world in cybersecurity, second only to the US globally.

Currently there are some 228 cybersecurity vendors in Israel, and only 15 in Australia. Israel has one third the population of Australia.

Meanwhile in the UK, and since the British government published its cybersecurity strategy in 2011, the cybersecurity sector in the UK has almost doubled from £10 billion to £17 billion and is now responsible for employing 100 thousand people.[49]

Australia can galvanise its own cybersecurity industry with government and private-sector support – but part of this involves addressing the need for more trained scientists, mathematicians, engineers, and ICT workers. As a nation we need a scientifically literate community capable of engaging in a national conversation on vital technology issues like cybersecurity.

Leveraging technology talent

Which leads us to the talent we already have – Australia has some of the world's top universities, but as a previously resource-driven economy we currently lack a technology focus, the type of which Israel recognised as essential for a data-driven future.

Collaboration of government, industry and research organisations to incentivise new developments and monetise research to bring products and services to market will be key. This includes interacting with incubators and accelerators, sharing key learnings from innovation, and encouraging entrepreneurial thinking.

Diversity is also a critical component in order to meet demand for skilled ICT workers. This includes utilising a greater proportion of our aged workforce, and galvanising interest in ICT with women, who are currently underrepresented in the technology sector (just 28% of ICT roles are held by women[50]) and represent a large untapped resource.

Challenges

Many of these devices are always on, always listening, and always communicating... raising concerns about transparency and privacy. With homeowners unprepared and ill-equipped to detect and remediate most security threats, some highly successful attacks will collect personal info on an ongoing basis.

McAfee Labs 2016 Threats Predictions[15]

While the opportunities are clear for ICT in Australia and the nation as a whole, there are a number of challenges we need to address. Ideally, all sectors from government and industry, to enterprise and academia, need to play a part in the development and promotion of cyber education, skills and products.

Leadership

Lack of leadership is a key challenge, if only because it takes a concerted effort to both recognise and take action on what is clearly a vital function in today's technologically savvy world.

This is true across government, the private sector, education and academia – the rate at which technology adoption occurs in Australia far outstrips our ability to predict the implications of technology, particularly when it comes to the results of cybercrime.

The foundation of any society is trust, as well as the foundation for security itself. Security helps build trust between people and technology. If we cannot protect for example personal data, it will have negative consequences for technology adoption and the ICT industry as a whole.

As a result, leadership is required to tackle issues around cybersecurity, governance, private-sector support and education to ensure we can adequately protect the foundation of trust upon which we all depend.

LEARNING FROM HISTORY

In 1958 when the National Defense Education Act was signed into law in the US, the goal was to provide funding to education institutions at all levels. The impetus was Russia beating the Americans to space, and a national feeling that America was falling behind. Over a period of four years $USD1 billion was spent on science education.[57]

Today we face a similar situation where we are already in a skills shortage for ICT in Australia, and if we are to create a blossoming cybersecurity ecosystem we will first need a strong emphasis on and promotion of STEM-based skillsets for Australians throughout the educational pathway.

695k

THE DEMAND FOR SKILLED ICT WORKERS WILL INCREASE FROM 638K TODAY TO 695K BY 2020

Collaboration

If there's one lesson to learn from cybercriminals it is this: collaboration is king. Analysis of attacks over the years has revealed that cybercriminals work together exceptionally well: sharing knowledge of exploits, selling stolen data in an open market, and working together to develop new hacking techniques for infiltration.

By contrast, compare this with the other side of the coin – those of us who defend against cyberattacks: siloed security vendors with competing products, little co-operation between government and industry, and companies afraid to share that they've been hacked for fear of impacting share price.

The latter is particularly important: knowledge is power, as we know, and so keeping a breach secret only helps the attackers – if an exploit isn't made public, it can be used on the next company, and the next. In order to stop it, free sharing of information among business and enterprise, cybersecurity professionals, and security software vendors is essential. As Ron Moritz of TrueBit Cyber Partners notes, "while industry remains separate, the bad guys will always be ahead."[52]

Therefore, developing the knowledge and software to protect against cyberattacks cannot happen in a vacuum. No one company or security vendor is able to withstand the collective might of an opponent who collaborates. This is a key lesson many in the private sector will have to learn if we are to keep pace in the cyber arms race.

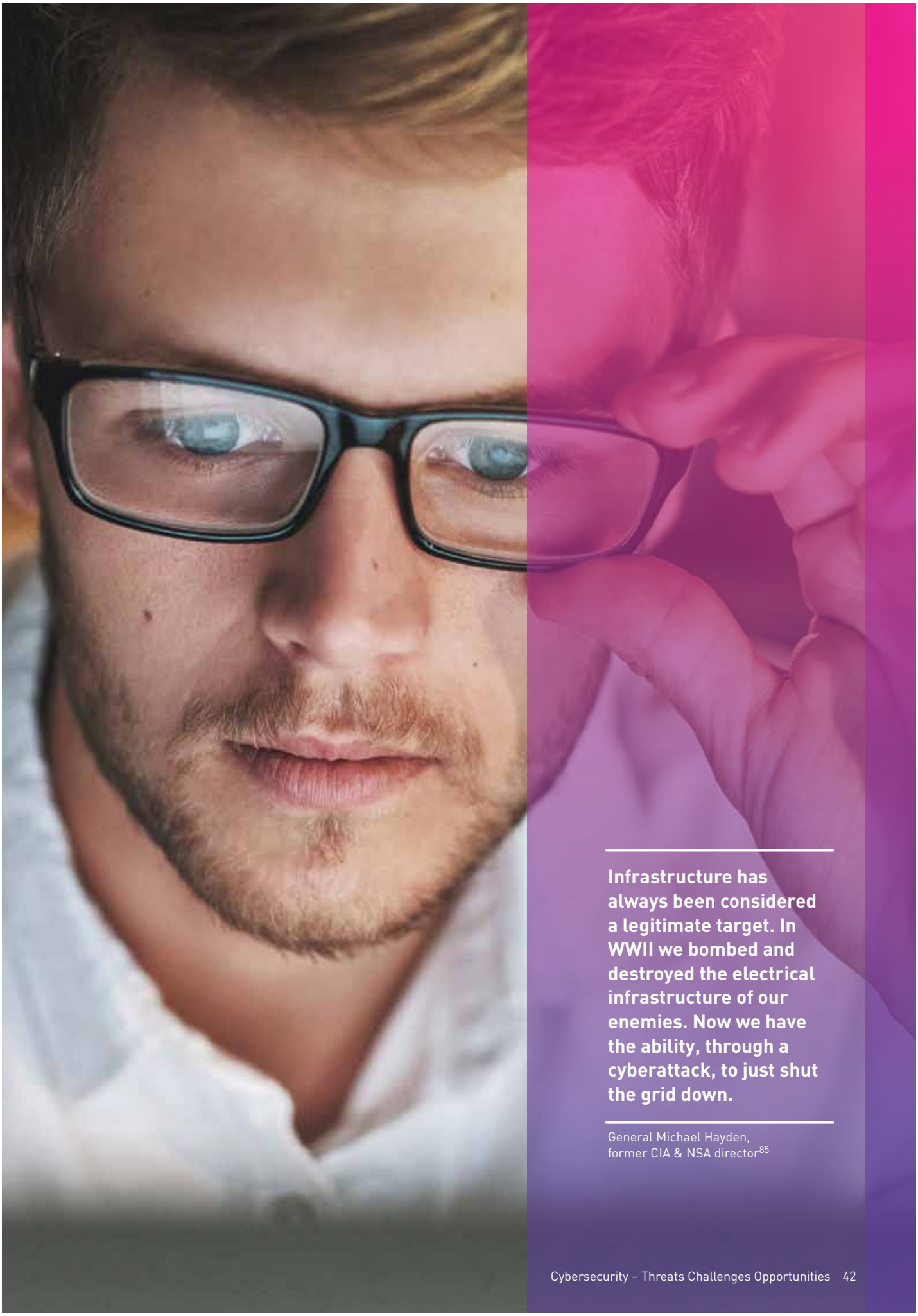
Education and awareness

According to **Australia's Digital Pulse**, a report commissioned by the ACS, the demand for skilled ICT workers will increase from 638K today to 695K by 2020, with ICT university graduates meeting only 1% of this demand.[50] Additionally, there has been a 35% drop in enrolment rates for ICT subjects at universities since 2001.[50]

As we move to a knowledge economy, we will need more scientists, mathematicians, engineers and programmers. Promotion and support of STEM subjects in schools, expanded degrees specific to cybersecurity disciplines at university, and an increased emphasis on entrepreneurial businesses skills will all help get Australians on track for roles in a cybersecurity industry as well as ICT at large.

It's interesting to note that professionals like lawyers and doctors are seen as prestigious, yet the skills and knowledge required to be a cybersecurity professional doesn't demand quite the same esteem. However, we are already at a stage where skilled cybersecurity professionals are essential to the operation of most industries in Australia. Can we generate a profession that garners a similar level of respect as other highly-skilled career paths?

Education also includes embedding cybersecurity in current workplace practice: as noted earlier, the weakest link is often people so good cybersecurity policies and



Infrastructure has always been considered a legitimate target. In WWII we bombed and destroyed the electrical infrastructure of our enemies. Now we have the ability, through a cyberattack, to just shut the grid down.

General Michael Hayden,
former CIA & NSA director[85]

YOU ARE WHAT YOU DO

The famous adage 'you are what you eat' has an interesting parallel in the digital world – it's easy to forget that almost anything you do online involves data, and that this data tells a story about who you are and where you have been. From web browsing to smartphones, you and everyone you know is tracked, logged, and the data shared among a variety of services.

Whether it's a connection from your IP address in a application's log, or cookies about a website stored on your computer, every day you leave a trail – often called your **digital exhaust** or **data exhaust**.

While much is for analytics, once it's out there you have no control over it, let alone ownership (most applications and programs will prompt you to sign over your permission on first use). Even Microsoft's latest Windows 10 comes with 'mandatory' data collection about your use of the operating system.

McAfee's 2016 Threats Predictions report notes that "within the next five years, the volume and types of personal information gathered and stored will grow from a person's name, address, phone number, email address, and some purchasing history to include frequently visited locations, 'normal' behaviours, what we eat, watch, and listen to, our weight, blood pressure, prescriptions, sleeping habits, daily schedule, and exercise routine."[15]

The more information that is out there about you, the greater the risk there is for it to be abused. Not just by cybercriminals seeking to develop correlations that can be used in fraud such as identity theft, but also intentional or unintentional misuse by companies or government services.

We're entering this world where everything is catalogued and everything is documented and companies and governments will be making decisions about you as an individual based on your data trail. If you want to be considered an individual and not just a data point, then it's in your interest to protect your privacy.

Josh Lifton, CEO of Crowd Supply[55]

procedures are as essential to the operation of any business. If you are in an organisation that currently does not have policies and procedures in place to both prevent and mitigate cybercrime, now is a good time to start.

Finally, perhaps the biggest hurdle here is educating the sector, particularly among CEOs and Boards. There is a dearth of knowledge among decision makers on cybersecurity risks and the investment required to manage them.

According to a survey by The Economist Intelligence Unit, IT and security leaders in Australia think cybersecurity is the #1 issue at present – but less than 6% of C-Suite executives agree. There is a large disconnect between the reality of threats and awareness of them at the executive level.[58]

Legal and regulatory

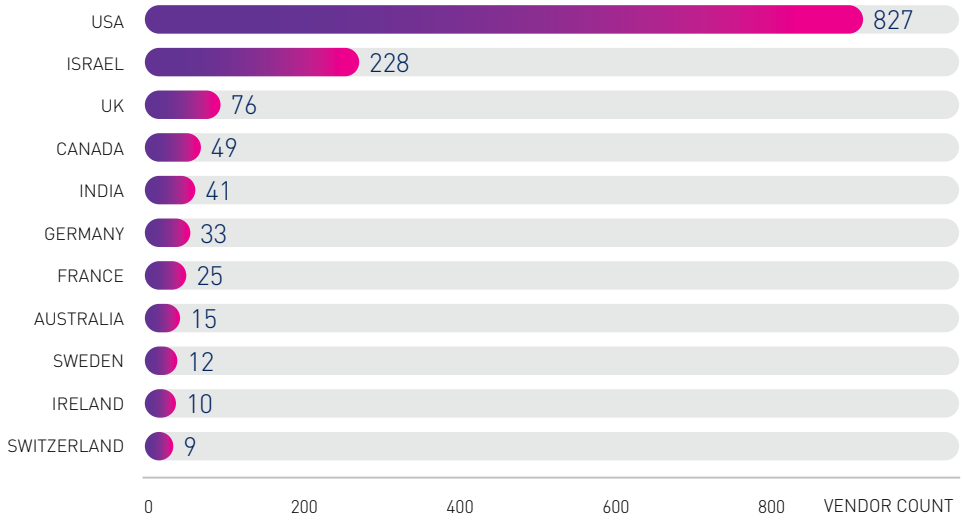
While collaboration is key, the good guys do have some hurdles the bad guys don't. For one, there may be legal or regulatory limitations, particularly where the sharing of information could breach privacy laws. Where necessary, reviewing laws and regulations to facilitate better communication and collaboration for the purposes of cybersecurity may be required.

Services and privacy

Increasingly in our digital world services come at the cost of privacy. There is an inherent trade-off, and while we accept some encroachment of privacy over data we share, it nonetheless remains a fundamental building block of our society and must factor into any solutions.

We now know there is no such thing as a 100% secure system, any personal data stored on any server be it government, enterprise, or otherwise has the possibility of being breached and personal information being made public.

It's also important to note how the type and volume of data stored also acts as a target for cybercrime, in cases of identity theft, for example. The trend today for many companies is to capture as much personal information as possible, all the better



CYBERSECURITY VENDORS BY COUNTRY AS AT 2016

USA and Israel currently lead cybersecurity research and products.
Source: IT-Harvest

to mine for advertising or other products, but as more breaches come to light this trade-off of personal data for services will come under increased scrutiny.

This has implications for mass surveillance and the storage of metadata. As Jill Slay, Director of the Australian Centre for Cyber Security, and Greg Austin, Professor Australian Centre for Cyber Security, succinctly noted, "you cannot demand mass surveillance and metadata retention without there being costs that make us much less safe. Metadata retention is retrospective – it won't predict or stop crimes, but it will open up breaches that bad actors can waltz through."[54]

The DDoS against the Australian Bureau of Statistics eCensus servers in August this year demonstrated just how easily a service can be knocked offline and, typically, DDoS attacks can often hide secondary attacks aimed at breaching a system. Any large database such as census data is a prime target for cybercriminals as it's a jackpot for identity theft. McAfee's Threats Predictions report for 2016 notes that "Government identity records such as birth/death, taxes, and national insurance IDs; and banking accounts and ATM transactions will also be targeted."[15]

Increasingly, as governments and corporations turn to big data, it will become paramount that this data be de-identified when possible to limit the damage from data breaches as well as preserve privacy of individuals.

Perception and practicality

Finally, there is a perception that Australia is not currently a technology leader – not just in cybersecurity, but as a whole. The current view with technological products is that it's better if it comes from overseas.[56]

This is a perception that needs to change. We have all the ingredients to create world-class products and services in Australia, particularly in relation to ICT and cybersecurity.

Pioneers like Atlassian and WiseTech Global demonstrate we have the capability to create highly successful companies and products that compete on the world stage.

Changing this perception will involve, in part, the promotion of the value of home-grown ICT and raising awareness of Australian technological solutions.

Practically, it also helps for the private sector and the ICT industry as a whole to seek Australian products when canvassing for solutions.

It's a market economy... the price of a compromised system of $5 shows you exactly how far down the road we are of the cybersecurity story.

Tim Wellsmore, Former Manager, Fusion Special Intelligence 2013-16[85]

Looking to the road ahead

It's clear cybersecurity is pivotal to both the economic future of Australia and indeed the fabric of our society. As we develop and embrace more and more technology, this will become ever more important.

For all my enthusiasm for government's responsibilities in cyberspace, good cyber policy requires the cooperation and creativity of academia and industry. Indeed, government needs to be challenged by academia and industry.

Malcolm Turnbull,
Prime Minister of Australia.
September 2016

Helping ensure a secure and successful environment ultimately comes down to every government, business, academic institution and individual around the world. All three are the targets of cybercrime and any government department, corporate network, or the smartphone in your pocket could be used as a vector for attack.

That's not to say we should all stop using technology because the risks are too high – it's all about process and procedure. Good government regulation, skilled and qualified IT staff in an organisation, and education about common scams and how to avoid them, can dramatically shrink the surface of exposure and minimise or prevent data breaches, cybercrime, and many of the threats covered here.

So what are other parts of the world doing, and what are we doing here in Australia?

State of the nation

Economies of scale aside, the US administration, under Obama and now Trump, allocated $US14 billion to cybersecurity spending in the 2016 budget[3], and has asked for $US19 billion for the 2017 fiscal year.[60]

In the UK the British Government has allocated £860 million over a five-year period from 2011-2016, and is increasing this to £1.9 billion to 2021.[51] The UK also conducts three exercises each month to test cyber resilience and response, and has a joint program with the US to prepare for a cyber-enabled terrorist attack on nuclear power stations. UK Chancellor George Osborne has called it "one of the greatest challenges of our lifetime".[54]

Elsewhere in Europe, the European Parliament in June imposed security and reporting obligations for industries such as "banking, energy, transport and health and on digital operators like search engines and online marketplaces."[87]

While in Japan the Japanese Government in August announced plans for a government institute, as part of Japan's Information Technology Promotion Agency (IPA), to train and educate employees to recognise and counter cyberattacks.[88]

So where are we now in Australia? In September this year Prime Minister Malcolm Turnbull addressed the Australia-US Cybersecurity Dialogue at the Center for Strategic and International Studies, in which he reiterated the importance of cybersecurity and noted "for all my enthusiasm for government's responsibilities in cyberspace, good cyber policy requires the cooperation and creativity of academia and industry. Indeed, government needs to be challenged by academia and industry."

On the 21st April, the Federal Government's Cyber Security Strategy[59] was launched and encompassed:

- A national cyber partnership between government, researchers and business including regular meetings to strengthen leadership and tackle emerging issues.

At the end of the day this really is about stewardship for us as a country. It's really about them, about the next generation. Bear in mind that they are only entrusting us with their future for a little while longer, because they're coming, and they're coming with or without us.

Adrian Turner, CEO, Data 61[93]

- Strong cyber defences to better detect, deter and respond to threats and anticipate risks.
- Working with international partners through the new Cyber Ambassador and other channels to champion a secure, open and free internet while building regional cyber capacity to crack down on cyber criminals and shut safe havens for cybercrime.
- Help Australian cybersecurity businesses to grow and prosper, nurturing our home-grown expertise to generate jobs and growth, and support new business models, markets and investment.
- Create more Australian cybersecurity professionals by establishing Academic Centres of Cyber Security Excellence in universities, fostering skills throughout the education system and raising awareness of cybersecurity.

Additionally, initiatives like the Australian Centre for Cyber Security, (now in its second year), and an injection of $30 million to establish an industry-led Cyber Security Growth Centre – charged with creating business opportunities for Australia's cybersecurity sector – as part of the National Innovation and Science Agenda further establishes the government's commitment to cybersecurity development in Australia.

Meanwhile, the CyCSA national Cyber Security Challenge (www.cyberchallenge.com.au) encourages students to participate in a cybersecurity competition. It's now in its fourth year.

What role can you play?

We know cybersecurity isn't just about technological defences; it's also about people and the way we handle data in the workplace, the emails we click or the sites we browse, and how good we are at identifying social engineering and other scams and tricks.

Good cybersecurity needs both good technological solutions and good people solutions. And, it requires all of us to participate.

In which case – whatever your responsibilities – what role can you play to make a difference?

Government

If you work in government, Prime Minister Malcolm Turnbull has already laid out in his address at the Australia-US Cyber Security Dialogue that leaders at government levels must know that "cyber is one of their essential functions" and to question what barriers can government "continue to remove, either through deregulation or positive action" to ensure the adoption of cybersecurity practices.

Regardless of your role in government, you can raise the conversation around cybersecurity and how it fits into your sector, and what the next steps are in bringing the government's cybersecurity strategy to fruition.

SHAKEN AND STIRRED

In security parlance a threat agent (not the 'James Bond' type) is an attack source combining motivation and capability. In general, threat agents can be categorised from benign to critical. To the right is a breakdown of common threat agent categories and their typical vectors:[25]

THREAT LEVEL	THREAT AGENT	THREAT VECTOR
CRITICAL	Nation state	Espionage, theft, sabotage, product alteration
	Competitor	Espionage, theft, product alteration
	Organised crime	Espionage, fraud, theft
	Terrorist	Sabotage, violence
HIGH	Activist/hacktivist	Espionage, data theft, sabotage
	Disgruntled employee	(All of the below)
	Reckless, untrained or distracted employees	Accidental breach or misuse of data
MEDIUM	Thief	Physical theft, espionage, fraud
	Irrational individual	Physical theft or sabotage
	Vendor or partner	Accidental leak, but also intentional fraud or theft
LOW	Outward sympathiser	Deliberate data leak or misuse of data

Education and research

If you work in academia, university, research or other educational institutions you have a great opportunity to see how cybersecurity principles can either be applied to your work, or considered in the application and delivery of your work.

Educational institutions from pre-school through to university all play a vital part in the promotion of STEM-based skills upon which disciplines such as cybersecurity are based. And, as we've noted in this guide, we are already in a shortage of skilled cybersecurity professionals. What you can do to promote this challenging and rewarding career pathway is of benefit not just to your students but Australia as a whole.

Within research and academic institutions the results of your work may be critical in any number of ways, and so if not already the access to and handling of data needs to be guided by solid cybersecurity principles in order to minimise or prevent any loss through a cyberattack.

Business and industry

In your workplace, the single most important step you can take is to draw attention to cybersecurity – or the lack of it – within your company. Write a cybersecurity report card looking at your organisation's policies, training and awareness programs, technical controls, management processes and general security culture.

Every business plays its part just as every one of us plays a part. The smartphone in your pocket could act as a vector for the theft of your own personal data, or as a vector of attack in the company you work for. It's in everyone's best interests to be informed, prepared, and responsible. Remember, cybersecurity is not just a safety risk, it's a business risk.

If you are an executive, it is incumbent on management to be well-versed in cybersecurity language and the realities of cybersecurity threats to your business. If not already, appoint a CISO (Chief Information Security Officer) or CSO (Chief Security Officer) and ensure they have a place in board-level decision making. Also ensure clear and easy lines of communication between security, IT staff and upper management – these employees are your front line of defence.

Remember that just as your business does not operate in a vacuum, the same is true for cybersecurity. You may have all the best policies and procedures in the world but be vulnerable through a third party such as suppliers or distributors with which you do business. It is important to ensure they, too, have adequate cybersecurity preparations and resources to protect themselves and the businesses they work with – and you can help them.

Finally, it's important to ensure your IT staff and security specialists are trained with up-to-date qualifications, as well as ensuring the have the necessary skills and expertise, and are certified to a recognised standard.

You, the individual

Because we all use a variety of devices every day, cybersecurity isn't just about protecting corporate networks or organisational assets. Each of us has plenty of data – personal information – that should remain personal and not be used against us for extortion, identity theft, or as part of a scam.

It's telling that we lock our doors when leave home, or lock our cars when we arrive at work, and yet don't consider the safety of the data on our computers when we browse the web or install an application.

And there's actually a lot you can do to help ensure your data remains yours. There are plenty of guides online, but a good summary includes:

- Use complex passwords over simple ones, and don't re-use passwords between sites and services. If you find passwords hard to remember, use a password manager.
- When on offer, use two-factor authentication. This is becoming more common now with various services to ensure others can't log in as you, even if they manage to attain your passwords.
- Learn to recognise phishing emails – listen to that nagging voice in your head: if it sounds suspicious, it is. Banks, government services, and reputable companies won't ask for your login details over email.
- Don't open files from someone you don't know, and don't download or install any files delivered through pop-ups or pop-unders during web browsing.
- Keep your operating system and your applications up-to-date with the latest patches.

There's plenty more to learn. See the Online Resources on page 52 for a good place to start.

The five pillars of cybersecurity readiness

As the peak body for ICT professionals in Australia, the ACS considers the following to be the five core pillars of cybersecurity readiness.

1

Education and Awareness

First and foremost, it's essential that cybersecurity forms part of the conversation in every organisation, from the lunch room to the boardroom. Only through keeping cybersecurity front of mind can it form part of the decision-making process, infrastructure investment, and regulatory and governance requirements.

Additionally, as people can themselves be an attack vector through social engineering, everyone within an organisation ultimately shares responsibility in ensuring best-practice cybersecurity processes are carried out. This requires staff education with regular updates to material as new threats arise. In fact, parallels have been drawn between cybersecurity and healthcare – everyone needs some form of cybersecurity education.

Finally, the employment of qualified cybersecurity professionals or certified training for key staff both in IT and management should form part of any cybersecurity readiness.

2

Planning and Preparation

A cybersecurity incident isn't an 'if' but a 'when', and to that end, preparation is essential. This can include management systems, best practice policies, IT auditing, and dedicated staff responsible for cybersecurity operations.

Good cybersecurity readiness encompasses an understanding of risks and threats to assets and information relevant to the organisation and its people, monitoring and detecting cybersecurity threats regularly, protecting critical systems and information, ensuring the organisation meets all relevant standards compliance, has incident response plans in place in the event of a breach, and clear business continuity plans to minimize any loss.

Typically, many of the above responsibilities belong to the CISO (Chief Information Security Officer) or equivalent, though other stake-holders such as senior leadership, legal and communications staff, and public relations may also need to have preparations in the event of an incident.

3

Detection and Recovery

When a breach happens, the quicker it is detected and responded to, the greater the chance of minimising loss – be it financial, reputational, or otherwise.

How quickly can your organisation identify and respond to the theft of data or the disabling of key services? How fast can affected servers or workstations be quarantined for forensic analysis? How quickly and easily can lost or corrupted data be restored? What is the incident response plan and who are the stakeholders that need to be notified immediately?

Importantly, the preservation and analysis of logs that can help identify how the breach happened, and thus how it can be closed, is part of the recovery process. It's not enough just to close the hole; an understanding of how the breach occurred can lead to preventing other, similar, breaches.

4

Sharing and Collaboration

As we've covered in this guide, collaboration is essential to mitigating current and future risks.

Sharing the results of your breach analysis with government and industry can help stop a known attack vector hitting other organisations. In turn, your company may be able to prevent an exploit by learning from a breach that another organisation shared.

Also consider joining or providing information to an ISAC (Information Sharing and Analysis Centers, www.nationalisacs.org) if there is an equivalent for your industry.

In some cases, your organisation may be bound by legislative requirements to report an incident. At a minimum, a breach should be reported to government or organisations such as AusCERT (www.auscert.org.au) and the Australian Centre for Cyber Security (www.acsc.gov.au).

5

Ethics and Certification

It may initially seem a less practical pillar, but the difference between a 'white hat' hacker and 'black hat' hacker is mindset.

In any company or organisation, ethics plays a role and should be of particular concern when it comes to cybersecurity. While some sectors, such as defence, will have their own means to vet credentials, for an industry as diverse and skilled as ICT it helps if professionals can demonstrate adherence to a code of ethics through membership of a professional institution.

Many professional organisations hold their members to standards that ensure the reputation and respectability of a profession is preserved. ACS, for example, has a code of ethics all Certified Professionals must abide by, in addition to other requirements such as demonstrating continued education and personal development in their chosen professional field of expertise.

ONLINE RESOURCES

For further reading and more information, visit the following websites:

- Australia's Cybersecurity Strategy **cybersecuritystrategy.dpmc.gov.au**
- Australian Center for Cyber Security **www.acsc.gov.au**
- Australian Computer Emergency Response Team (AusCERT) **www.auscert.org.au**
- Australian Cybercrime Online Reporting Network (ACORN) **www.acorn.gov.au**
- Australian Internet Security Initiative **www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative**
- Australian Signals Directorate – Top 4 Mitigation Strategies **www.asd.gov.au/infosec/mitigationstrategies.htm**
- Australian Signals Directorate – CyberSense Videos **www.asd.gov.au/videos/cybersense.htm**
- Australian Government – Stay Smart Online **www.staysmartonline.gov.au**
- ACCC – Scam Watch **www.scamwatch.gov.au**
- Australian Computer Society (ACS) **www.acs.org.au**

Through the looking glass

The following is a snapshot – just a sample – of the stories that made the news during the production of this guide. These headlines give you an insight to the ongoing, every day, occurrences of what happens in the absence of cybersecurity.

'LINKEDIN USER? YOUR DATA MAY BE UP FOR SALE'[61]

'EASYDOC MALWARE ADDS TOR BACKDOOR TO MACS FOR BOTNET CONTROL'[63]

'LIZARDSTRESSER BOTNETS USING WEBCAMS, IOT GADGETS TO LAUNCH DDOS ATTACKS'[65]

'DDOS ATTACK TAKES DOWN US CONGRESS WEBSITE FOR THREE DAYS'[67]

'HACKERS FIND 138 SECURITY GAPS IN PENTAGON WEBSITES'[69]

'HACKER STEALS 45 MILLION ACCOUNTS FROM HUNDREDS OF CAR, TECH, SPORTS FORUMS'[71]

'10 MILLION ANDROID DEVICES REPORTEDLY INFECTED WITH CHINESE MALWARE'[73]

'THIEVES GO HIGH-TECH TO STEAL CARS'[75]

'CROOKS ARE WINNING THE 'CYBER ARMS RACE', ADMIT COPS'[77]

The US government has increased its annual cybersecurity budget by 35%, going from $14 billion budgeted in 2016 to $19 billion in 2017. This is a sign of the times and there's no end in sight. Incremental increases in cybersecurity spending are not enough. We expect businesses of all sizes and types, and governments globally, to double down on cyber protection.

Cybersecurity Ventures[48]

'A HACK WILL KILL SOMEONE WITHIN 10 YEARS AND IT MAY HAVE ALREADY HAPPENED'[79]

'CHINA HACKED US BANKING REGULATOR'[81]

'APPLE DEVICES HELD FOR RANSOM, RUMOURS CLAIM 40M ICLOUD ACCOUNTS HACKED'[62]

'RESEARCHERS DISCOVER TOR NODES DESIGNED TO SPY ON HIDDEN SERVICES'[64]

'RESEARCHERS FOUND A HACKING TOOL THAT TARGETS ENERGY GRIDS ON THE DARK WEB'[66]

'CITING ATTACK, GOTOMYPC RESETS ALL PASSWORDS'[68]

'POLITICAL PARTY'S VIDEO CONFERENCE SYSTEM HACKED, ALLOWED SPYING ON DEMAND'[70]

'ONLINE BACKUP FIRM CARBONITE TELLS USERS TO CHANGE THEIR PASSWORDS NOW'[72]

'ANDROID RANSOMWARE HITS SMART TVS'[74]

'HACKERS CAN USE SMART WATCH MOVEMENTS TO REVEAL A WEARER'S ATM PIN'[76]

'IDENTITY FRAUD UP BY 57% AS THIEVES 'HUNT' ON SOCIAL MEDIA'[78]

'WHY YOU SHOULD DELETE THE ONLINE ACCOUNTS YOU DON'T USE ANYMORE – RIGHT NOW'[80]

'MASSIVE DDOS ATTACKS REACH RECORD LEVELS'[28]

'HACKER DEMONSTRATES HOW VOTING MACHINES CAN BE COMPROMISED'[89]

'FTC WARNS CONSUMERS OF RENTAL CAR DATA THEFT RISK'[90]

'YAHOO CONFIRMS MASSIVE DATA BREACH, 500 MILLION USERS IMPACTED'[91]

Fast facts

It's hard to choose just a handful of facts that highlight the threats and opportunities facing Australia, but here is a sample.

THREATS

IN 2014-15 CERT (COMPUTER EMERGENCY RESPONSE TEAM) AUSTRALIA RESPONDED TO

11,733

INCIDENTS, 218 OF WHICH INVOLVED SYSTEMS OF NATIONAL INTEREST OR CRITICAL INFRASTRUCTURE. OF THESE, ENERGY, BANKING AND FINANCE, AND COMMUNICATIONS WERE THE TOP THREE TARGETS.[82]

THE AUSTRALIAN GOVERNMENT DEPARTMENT OF COMMUNICATIONS HAS REPORTED THAT THE AVERAGE COST OF A CYBERCRIME ATTACK TO A BUSINESS IS AROUND

$276,000[92]

THE WORLD ECONOMIC FORUM'S GLOBAL RISKS 2015 REPORT HIGHLIGHTED CYBERATTACKS AND THREATS AS ONE OF THE MOST LIKELY HIGH-IMPACT RISKS. IN THE UNITED STATES, FOR EXAMPLE, CYBER CRIME ALREADY COSTS AN ESTIMATED

$US100

BILLION A YEAR.[50]

IOT SENSORS AND DEVICES ARE EXPECTED TO EXCEED MOBILE PHONES AS THE LARGEST CATEGORY OF CONNECTED DEVICES IN 2018, GROWING AT A

23%

COMPOUND ANNUAL GROWTH RATE (CAGR) FROM 2015 TO 2021.[83] SOLID CYBERSECURITY POLICY MUST BE IN PLACE FOR THIS FUTURE.

CYBERSECURITY IS A BUSINESS ISSUE, NOT JUST A TECHNOLOGY ONE. IN A SURVEY OF CLOSE TO

4,000

COMPANY DIRECTORS IN AUSTRALIA, ROUGHLY ONLY HALF REPORTED TO BE CYBER LITERATE, AND OF CO-DIRECTORS ONLY

FIFTEEN

PERCENT CLASSED AS CYBER LITERATE. THERE IS A LACK OF KNOWLEDGE ABOUT CYBERSECURITY AT THE EXECUTIVE LEVEL IN MANY BUSINESSES IN AUSTRALIA.[1]

OPPORTUNITIES

IN 2003 THE CYBERSECURITY INDUSTRY WAS TAGGED AT

$US2.5

BILLION TODAY THE GLOBAL CYBERSECURITY MARKET TOTALS MORE THAN $US106 BILLION. SOME ESTIMATES PEG THE SECTOR WILL BE WORTH $US639 BILLION BY 2023.[1]

BY 2030 IT'S ESTIMATED DATA ANALYTICS, MOBILE INTERNET, CLOUD AND IOT COULD GENERATE $US625

BILLION

IN SALES PER YEAR IN APAC.[1]

THE UK PUBLISHED ITS CYBER-SECURITY STRATEGY IN 2011 – SINCE THEN THE SECTOR ALMOST DOUBLED FROM TEN BILLION POUNDS TO

SEVENTEEN

BILLION POUNDS AND IS NOW RESPONSIBLE FOR EMPLOYING 100K PEOPLE.[51]

THERE ARE

1,404

CYBERSECURITY VENDORS IN THE WORLD TODAY. AUSTRALIA SPORTS ONLY FIFTEEN. VENDORS BY COUNTRY: USA 827, ISRAEL 228, UK 76, INDIA 41, AUSTRALIA 15.[1]

JOB ADVERTISEMENTS FOR CYBER-SECURITY ALONE HAVE GROWN

57%

IN THE LAST 12 MONTHS ACCORDING TO JOBS WEBSITE SEEK. NETWORK SECURITY CONSULTANTS WERE THE

SIXTH

MOST ADVERTISED ICT OCCUPATION ON LINKEDIN IN 2015.[50]

Glossary

A collection of some common words and phrases you will see used for discussions in and around cybersecurity.

Administrator: Person who administers a computer system or network and has access to the Administrator account.

Black Hat: Programmers who 'hack' into systems to test their capabilities, and exploit vulnerabilities for personal or financial gain. See Cybercrime.

Advanced Persistent Threat: Usually refers to long-term stealth attacks on or infiltration of a system, but can also be used to describe a group, such as a foreign government, with advanced cyberattack capabilities.

CIO/CISO: Chief Information Officer/ Chief Information Security Officer. Executive position responsible for ensuring the security of systems and data in an organisation (can include physical security).

Critical infrastructure: Physical and virtual assets that are vital to the operation of an organisation or nation, for example, the electrical grid.

Cyberattack: An offensive act against computer systems, networks, or infrastructure.

Cybercrime: Computer-facilitated crimes, though frequently can be used to refer to all forms of technology-enabled crimes.

Cyberespionage: The practice and theft of confidential information from an individual or organisation.

Cybersecurity: The discipline and practice of preventing and mitigating attacks on computer systems and networks.

Cyberthreat: A potential threat targeting computer systems and technology, typically from the internet.

Cyberwarfare: Internet-based conflict to attack computer systems to disrupt or destroy. Usually in reference to nation states but can also refer to companies, terrorist or political groups, or activists.

DoS/DDoS: Denial of Service/ Distributed Denial of Service. A common attack involving thousands of devices accessing a site simultaneously and continually to overload its ability to serve web pages.

Hacker/Hacking: While originally in reference to a programmer 'hacking at code', it's now become mainstream to represent individuals who maliciously breach ('hack into') computers and related systems.

ICT: Information and Communications Technology. Overarching term encompassing all forms of computing and telecommunications technology inclusive of hardware, software, and networks.

IoT: Internet of Things. An evolving definition of the wide-variety of internet-connected devices ranging from sensors to smartphones.

Internet security: A general term referring to the security of internet-related technologies, such as web browsers, but also that of the underlying operating system or networks.

Malware: Catch-all term to refer to any type of malicious software, typically used in reference to viruses, ransomware, spyware and similar.

Phishing: Deceptive attempt, usually over email, to trick users into handing over personally identifiable or critical information (such as passwords or credit card numbers). A form of social engineering.

Ransomware: Malware used to hold an individual or organisation to ransom, typically by encrypting files or an entire hard drive and demanding payment to 'unlock' the data. Also known as Cryptoware.

Social engineering: The practice of manipulating human beings to gain access to data or computer systems.

Spear-phishing: Highly-targeted form of phishing towards an individual or business, often utilising social engineering techniques to appear to be from a trusted source.

Spyware: Covert software designed to steal data or monitor people and systems for cybercriminals, organisations, or nation states.

Threat actor: an individual or entity that has the potential to impact, or has already impacted, the security of an organisation.

White Hat: Programmers who 'hack' into systems to test their capabilities, and report vulnerabilities to authorities to be fixed.

References

05

1 Richard Stiennon, Chief Research Analyst, IT-Harvest,
National Fintech Cybersecurity Summit 2016

2 Internet Users by Country 2016, Internet Life Stats, July 2016
www.internetlivestats.com/internet-users-by-country

3 'Cybersecurity Market... Expected To Reach $170 Billion By 2020', Forbes, Dec 2015
www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020

4 'One in two users click on links from unknown senders', Fau.eu, August 2016
www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders

5 'Biggest cybersecurity threats in 2016', CNBC, Dec 2015
www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html

6 'Hackers remotely kill a jeep on the highway', Wired, July 2015
www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

7 'Hackers can send fatal dose to hospital drug pumps', Wired, June 2015
www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps

8 'Hackers can hijack Wi-Fi Hello Barbie to spy on your children', The Guardian, November 2015
www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children

9 Simi Bajaj, 'Cyber Fraud: A Digital Crime',
www.academia.edu/8353884/cyber_fraud_a_digital_crime

10 Akamai's State of the Internet Security Report Q2 2015
media.scmagazine.com/documents/144/q2_2015_soti_security_report_-_35820.pdf

11 Contracting for the Internet of Things: Looking into the Nest,
Social Science Research Network, February 2016
ssrn.com/abstract=2725913

12 'Cisco CEO Pegs Internet of Things as $19 Trillion Market',
Bloomberg Technology, January 2014
www.bloomberg.com/news/articles/2014-01-08/cisco-ceo-pegs-internet-of-things-as-19-trillion-market

13 'Aussie IoT in the home spend tipped to top $200m in 2020', IoT Australia, November 2015
www.iotaustralia.org.au/2015/11/06/iot-facts-and-forecasts/aussie-iot-in-the-home-spend-tipped-to-top-200m-in-2020

14 A guide to the Internet of Things Infographic, Intel
www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

15 2016 Threats Predictions, McAfee Labs, 2016
www.mcafee.com/au/resources/reports/rp-threats-predictions-2016.pdf

16 'Lax Security Opens the Door for Mass-Scale Abuse', Imperva Incapsula, May 2015
www.incapsula.com/blog/ddos-botnet-soho-router.html

References continued

17 'Hosting company OVH suffers world's largest 1 Tbps DDoS attack', TheTechPortal.com
thetechportal.com/2016/09/28/worlds-largest-ddos-attack-ovh-iot

18 Dissecting the Top Five Network Attack Methods: A Thief's Perspective,
McAfee & Intel Security, 2015
www.mcafee.com/us/resources/reports/rp-dissecting-top-5-network-methods-thiefs-perspective.pdf

19 'The Lizard Brain of Lizard Stresser', Arbor Networks, June 2016
www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser

20 'BMW, Mercedes Vulnerable to Remote-Unlocking Hack', Car and Driver, August 2015
blog.caranddriver.com/researcher-bmw-mercedes-vulnerable-to-remote-unlocking-hack

21 'BMW, Audi and Toyota cars can be unlocked and started with hacked radios',
The Telegraph UK, April 2016.
www.telegraph.co.uk/technology/2016/03/23/hackers-can-unlock-and-start-dozens-of-high-end-cars-through-the

22 'Fiat Chrysler recalls 1.4 million cars after Jeep hack', BBC News, July 2015
www.bbc.com/news/technology-33650491

23 The Connected Car Report, Business Insider, March 2015
www.businessinsider.com.au/connected-car-forecasts-top-manufacturers-leading-car-makers-2015-3

24 'Mark Zuckerberg covers his laptop camera and you should too',
Australian Financial Review, June 2016.
www.afr.com/technology/web/security/mark-zuckerberg-covers-his-laptop-camera-and-you-should-too-20160623-gppvwy

25 Critical Infrastructure Readiness Report, The Aspen Institute & Intel Security, 2015
www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf

26 Identity Theft Prevention – ID Theft Facts and Figures 2016, Kaspersky Lab, May 2016
youtu.be/Fztuohj3Fck

27 'The Next Wave of Cyberattacks Won't Steal Data -- They'll Change It',
Defense One, September 2015
www.defenseone.com/threats/2015/09/next-wave-cyberattacks-wont-steal-data-theyll-change-it/120701

28 'Massive DDoS attacks reach record levels as botnets make them cheaper to launch',
Network World, June 2016
www.networkworld.com/article/3079987/massive-ddos-attacks-reach-record-levels-as-botnets-make-them-cheaper-tolaunch.html

29 Therac-25, Wikipedia, 2016
en.wikipedia.org/wiki/Therac-25

30 'The Patriot Missile Failure', Douglas Arnold, August 2000
ima.umn.edu/~arnold/disasters/patriot.html

31 'Toyota's killer firmware: bad design and its consequences', EDN Network, October 2013
www.edn.com/design/automotive/4423428/Toyota-s-killer-firmware--Bad-design-and-its-consequences

32 'Tesla Autopilot Enthusiast Killed In First Self-Driving Car Death', Forbes, June 2016
www.forbes.com/sites/briansolomon/2016/06/30/the-first-self-driving-car-death-launches-tesla-investigation/

33 'Chinese cyberattacks hit key US weapons systems. Are they still reliable?', Christian Science Monitor, May 2013
www.csmonitor.com/USA/Military/2013/0528/Chinese-cyberattacks-hit-key-US-weapons-systems.-Are-they-still-reliable

34 'Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors', Wired, December 2015
www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors

35 'The 10 Commandments of Data Sovereignty', CSO Online, July 2013
www.cso.com.au/article/466539/10_commandments_data_sovereignty

36 'Russia Imposes New Data Storage Requirements for Telecoms and ISPs', Hogan Lovells Media, July 2016
www.hlmediacomms.com/2016/07/11/russia-imposes-new-data-storage-requirements-for-telecoms-and-isps

37 'We are removing our Russian presence', PrivateInternetAccess.com
www.privateinternetaccess.com/forum/discussion/21779/we-are-removing-our-russian-presence

38 Image, Cyber Security Trends 2016, Cybernetic Global Intelligence, November 2015
cgi-content-imagesandcode.cyberneticglobal.netdna-cdn.com/wp-contentuploads/2015/11/cyber-predictions-2016-v2.png

39 Russo-Georgian War, Wikipedia, 2016
en.wikipedia.org/wiki/Russo-Georgian_War

40 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', Wired, November 2014
www.wired.com/2014/11/countdown-to-zero-day-stuxnet

41 'A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever', Wired, January 2015
www.wired.com/2015/01/german-steel-mill-hack-destruction

42 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', Wired, March 2016.
www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid

43 French Coldwell, Chief Evangelist, Metricstream,
National Fintech Cybersecurity Summit 2016, Sydney

44 'Kaspersky report on Energetic Bear', Security Affairs, August 2014
securityaffairs.co/wordpress/27224/cyber-crime/kaspersky-report-energetic-bear.html

45 ''Mayhem' program wins grand hacking challenge', BBC News, August 2016
www.bbc.com/news/technology-36980307

46 'When Paying Out Doesn't Pay Off', Talos Intel, July 2016
blog.talosintel.com/2016/07/ranscam.html

47 Fintech 100: Nine Australian companies make the cut
www.home.kpmg.com/au/en/home/media/press-releases/2016/10/the-fintech-100-announcing-the-worlds-leading-fintech-innovators-for-2016.html

48 Cybersecurity Market Report, Cybersecurity Ventures, 2016
cybersecurityventures.com/cybersecurity-market-report

49 Chancellor's speech to GCHQ on cyber security
www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

References continued

50 Australia's Digital Pulse 2016, ACS & Deloitte Access Economics
www.acs.org.au/content/dam/acs/acs-documents/PJ52569-Australias-Digital-Pulse-2016_LAYOUT_Final_Web.pdf

51 The UK Cyber Security Strategy 2011-2016, Annual Report, April 2016
www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

52 Ron Moritz, TrueBit Cyber Partners, National Fintech Cybersecurity Summit 2016, Sydney

53 Email interview, Rodney Gedda Senior Analyst, Telsyte, July 2016

54 'The Australian government must take cyber security more seriously', The Conversation, June 2016
theconversation.com/the-australian-government-must-take-cyber-security-more-seriously-60231

55 The dark side of wearables: How they're secretly jeopardizing your security and privacy, Tech Republic, April 2016
www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/

56 Alex Scundurra, CEO Stone & Chalk, National Fintech Cybersecurity Summit 2016, Sydney

57 National Defense Education Act, Wikipedia, 2016
en.wikipedia.org/wiki/National_Defense_Education_Act

58 'The cyber-chasm: How the disconnect between the C-suite and security endangers the enterprise'
www.vmware.com/radius/wp-content/uploads/2015/08/EIU-VMware-Data-Security-Briefing.pdf

59 Australia's Cybersecurity Strategy, Commonwealth of Australia, Department of the Prime Minister and Cabinet, 2016
cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

60 'Concerned by cyber threat, Obama seeks big increase in funding', Reuters, February 2016
www.reuters.com/article/us-obama-budget-cyber-idUSKCN0VI0R1
516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf
theconversation.com/the-australian-government-must-take-cyber-security-more-seriously-60231

61 'LinkedIn user? Your data may be up for sale', ZDNet, May 2016
www.zdnet.com/article/linkedin-user-millions-of-users-data-is-up-for-sale

62 'Apple devices held for ransom', CSO Online, July 2016
www.csoonline.com/article/3093016/security/apple-devices-held-for-ransom-rumors-claim-40m-icloud-accounts-hacked.html

63 'EasyDoc malware adds Tor backdoor to Macs for botnet control', The Register, July 2016
www.theregister.co.uk/2016/07/05/easydoc_malware_adds_tor_backdoor_to_mac_systems_for_botnet_control/

64 'Researchers Discover Tor Nodes Designed to Spy on Hidden Services', Schneier on Security, July 2016
www.schneier.com/blog/archives/2016/07/researchers_dis.html

65 'LizardStresser botnets using webcams, IoT gadgets to launch DDoS attacks', SC Magazine, July 2016
www.scmagazineuk.com/lizardstresser-botnets-using-webcams-iot-gadgets-to-launch-ddos-attacks/article/506962

66 'Researchers Found a Hacking Tool that Targets Energy Grids on the Dark Web', Motherboard, July 2016
motherboard.vice.com/read/researchers-found-a-hacking-tool-that-targets-energy-grids-on-dark-web-forum

67 'DDoS Attack Takes Down US Congress Website for Three Days', Softpedia News, July 2016
news.softpedia.com/news/ddos-attack-takes-down-us-congress-website-for-three-days-506451.shtml

68 'Citing Attack, GoToMyPC Resets All Passwords', Krebs On Security, June 2016
krebsonsecurity.com/2016/06/citing-attack-gotomypc-resets-all-passwords

69 'Hackers Find Security Gaps in Pentagon Websites', ABC News, June 2016
abcnews.go.com/Technology/wireStory/hackers-find-security-gaps-pentagon-websites-39945560

70 'Political Party's Videoconference System Hacked, Allowed Spying On Demand', Slashdot, June 2016
news.slashdot.org/story/16/06/18/1831235/political-partys-videoconference-system-hacked-allowed-spying-on-demand

71 'Hacker steals 45 million accounts from hundreds of car, tech, sports forums', ZDNet, June 2016
www.zdnet.com/article/hacker-steals-45-million-accounts-from-hundreds-of-verticalscope-car-tech-sports-forums/

72 'Online Backup Firm Carbonite Tells Users To Change Their Passwords Now', Slashdot, June 2016
it.slashdot.org/story/16/06/21/2032209/online-backup-firm-carbonite-tells-users-to-change-their-passwords-now

73 '10 million Android devices reportedly infected with Chinese malware', CNet, July 2016
www.cnet.com/news/malware-from-china-infects-over-10-million-android-users-report-says

74 'FLocker Mobile Ransomware Crosses to Smart TV', Trend Micro, June 2016
yro.slashdot.org/story/16/06/13/1845221/android-ransomware-hits-smart-tvs

75 'Thieves Go High-Tech to Steal Cars', The Wall Street Journal, July 2016
www.wsj.com/articles/thieves-go-high-tech-to-steal-cars-1467744606

76 'Hackers Can Use Smart Watch Movements To Reveal A Wearer's ATM PIN', Slashdot, July 2016
news.slashdot.org/story/16/07/06/2132206/hackers-can-use-smart-watch-movements-to-reveal-a-wearers-atm-pin

77 'Crooks are winning the 'cyber arms race' admit cops', ZDNet, July 2016
www.zdnet.com/article/crooks-are-winning-the-cyber-arms-race-admit-cops

78 'Identity fraud up by 57% as thieves 'hunt' on social media', BBC News, July 2016
www.bbc.com/news/uk-36701297

79 'A hack will kill someone within 10 years and it may have already happened', Yahoo News, June 2016
uk.news.yahoo.com/hack-kill-someone-within-10-091800465.html

References continued

80 'Why you should delete the online accounts you don't use anymore - right now', Sydney Morning Herald, June 2016. www.smh.com.au/technology/technology-news/why-you-should-delete-the-online-accounts-you-dont-use-anymore--right-now-20160602-gp9n18.html

81 'China Hacked US Banking Regulator From 2010 Until 2013', Slashdot, July 2016 yro.slashdot.org/story/16/07/13/1923215/china-hacked-us-banking-regulator-from-2010-until-2013---and-us-officials-covered-itup-report

82 2015 Threat Report, Australian Cyber Security Centre, 2015 www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

83 'Internet Of Things On Pace To Replace Mobile Phones As Most Connected Device In 2018', Forbes, July 2016 www.forbes.com/sites/louiscolumbus/2016/07/09/internet-of-things-on-pace-to-replace-mobile- phones-as-most-connecteddevice-in-2018/#468e81846aef

84 'One of Europe's Biggest Companies Loses €40 Million in Online Scam', Softpedia news.softpedia.com/news/one-of-europe-s-biggest-companies-loses-40-million-in-online-scam-507818.shtml

85 Cyber War, ABC, 4 Corners, August 2015 www.abc.net.au/4corners/stories/2016/08/29/4526527.htm

86 'Robot Lawyers Could Make Time-Consuming, Expensive Court Conflict Thing Of The Past', ABC, July 2016 www.abc.net.au/news/2016-07-06/robot-lawyers-dutch-conflict-resolution-technology-on-its-way/7572488

87 'European Union's First Cybersecurity Law Gets Green Light', Bloomberg Technology, July 6 www.bloomberg.com/news/articles/2016-07-06/european-union-s-first-cybersecurity-law-gets-green-light

88 'Japanese Government Plans Cyber Attack Institute', The Stack, August 2016 thestack.com/security/2016/08/24/japanese-government-plans-cyber-attack-institute

89 'Hacker Demonstrates How Voting Machines Can Be Compromised', CBS News, August 2016 www.cbsnews.com/news/rigged-presidential-elections-hackers-demonstrate-voting-threat-old-machines

90 'FTC Warns Consumers: Don't Sync To Your Rental Car!', Slashdot, September 2016 tech.slashdot.org/story/16/09/04/0912201/ftc-warns-consumers-dont-sync-to-your-rental-car

91 'Yahoo Confirms Massive Data Breach, 500 Million Users Impacted', Slashdot, September 2016 it.slashdot.org/story/16/09/22/095255/yahoo-confirms-massive-data-breach-500-million-users-impacted-updated

92 Image, StaySmartOnline.gov.au, October 2015 www.staysmartonline.gov.au/sites/g/files/net301/f/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf

93 Adrian Turner, CEO, Data 61, National Fintech Cybersecurity Summit 2016, Sydney

ABOUT THE ACS

The Australian Computer Society is the professional association for Australia's Information and Communications Technology sector.

We are passionate about recognising and developing ICT skills and provide more than 60 products and services to our members. We are also the voice of Australian ICT, representing all practitioners in business, government and education.

In everything we do, our goal is to advance ICT in Australia and help our members be the best they can be.

COPYRIGHT NOTICE

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

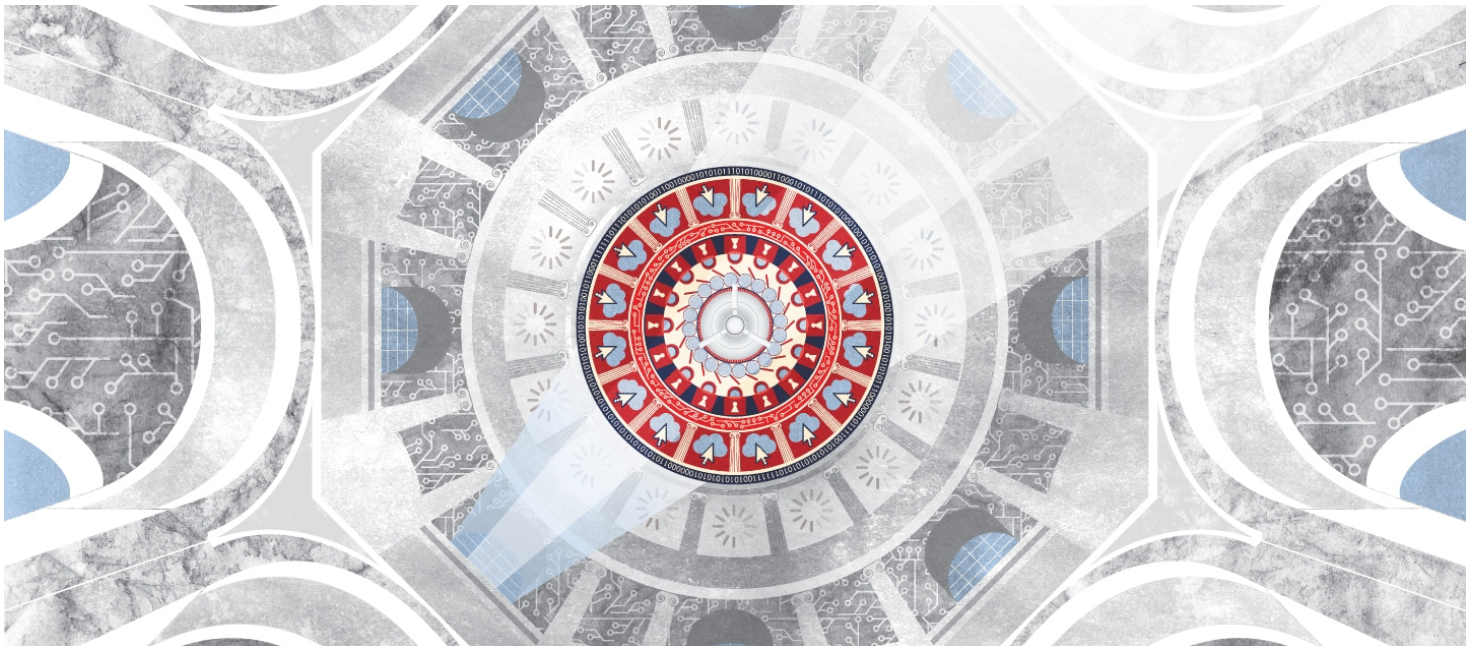
creativecommons.org/licenses/by-sa/4.0

ACS
Level 11
50 Carrington Street
Sydney NSW 2000

P: 02 9299 3666
F: 02 9299 3997
E: info@acs.org.au
W: www.acs.org.au

Deloitte-NASCIO
Cybersecurity Survey

September 2016



Article

2016 Deloitte-NASCIO Cybersecurity Study

State governments at risk: Turning strategy and awareness into progress

Doug Robinson < https://dupress.deloitte.com/dup-us-en/authors/r/doug-robinson.html> , Srini Subramanian < https://dupress.deloitte.com/dup-us-en/authors/s/srini-subramanian.html>

September 20, 2016

For state governments, many challenges of managing cyber risk—in both funding and talent—have persisted over the years. Yet states have also made progress, as governor-level awareness rises

and CISOs make strides in collaborating with other government agencies.

Foreword

Today, no one disputes that state governments need to be concerned with cyber risk. The 2016 Deloitte-NASCIO Cybersecurity Study shows that cyber risk has risen in importance in the eyes of governors and other state executives. For CIOs and CISOs, this governor-level attention is encouraging news and an opportunity to secure resources and support for state cybersecurity programs.

Given its current trajectory, cyber risk in state governments is unlikely to dissipate, and may even grow—largely a result of the increase in innovation and use of technology and data. State governments have rapidly adopted new technology to better serve constituents and reduce dependency on legacy systems that are difficult to maintain. Ironically, the very steps governments have taken to embrace these new innovations add to the cyber risks. This is why we need to begin viewing the management of cyber risk as a core function of running government operations.

Since 2010, Deloitte and NASCIO have been conducting biennial surveys of CISOs and state officials to explore how states are managing cyber risk. In our fourth survey to date, we found that even as the importance of cybersecurity has gained ascendancy, many of the issues CISOs are grappling with are stubbornly persistent. Following are some of the top takeaways from the 2016 survey:

Governor-level awareness is on the rise. The survey results indicate that governors and other state officials are receiving more frequent reports from CIOs/CISOs. Initiatives such as the National Governors Association (NGA) "Call to Action" seem to be helping to maintain the prominence of cybersecurity on executive agendas.

Cybersecurity is becoming part of the fabric of government operations. For the first time, all respondents report having an enterprise-level CISO position. The CISO role itself has become more consistent in terms of responsibilities and span of oversight. CISOs are also focusing their energies more on what they can control.

A formal strategy and better communications lead to greater command of resources . Securing sufficient resources—both funding and talent—remains a top challenge for CISOs. This year, we found evidence that states that take a proactive approach to strategy setting and communication are more likely to see improvements in funding and access to talent.

We believe that, overall, the survey results spell out a clear message for CISOs: **State leaders are paying attention. Take advantage of this focus to make substantial progress.**

Finally, we would like to thank participants in this year's survey: the 49 CISOs who responded to the longer version of the survey—24 of whom were new to their role—and the 96 state officials who responded to the accompanying state officials survey. Your time and commitment will help states in their efforts to effectively manage

cyber risk and protect citizen data.

The authors of the survey,

Doug Robinson

Executive Director

NASCIO

Srini Subramanian

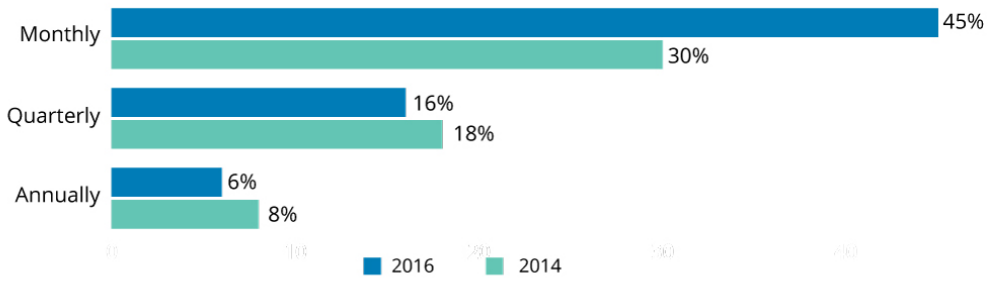
Principal

Deloitte & Touche LLP

Governor-level awareness is on the rise

The critical nature of cybersecurity has not been lost on governors and other state officials. The state officials survey this year shows that over 90 percent say that cybersecurity is important to their state, and over 94 percent say that it is important to their individual agency. Cybersecurity is also a more frequent topic of discussion at state executive leadership meetings (figure 1). More than three-fifths (61 percent) of state officials say that cybersecurity is discussed at executive leadership meetings at least quarterly, if not monthly, compared with less than half (48 percent) in 2014.

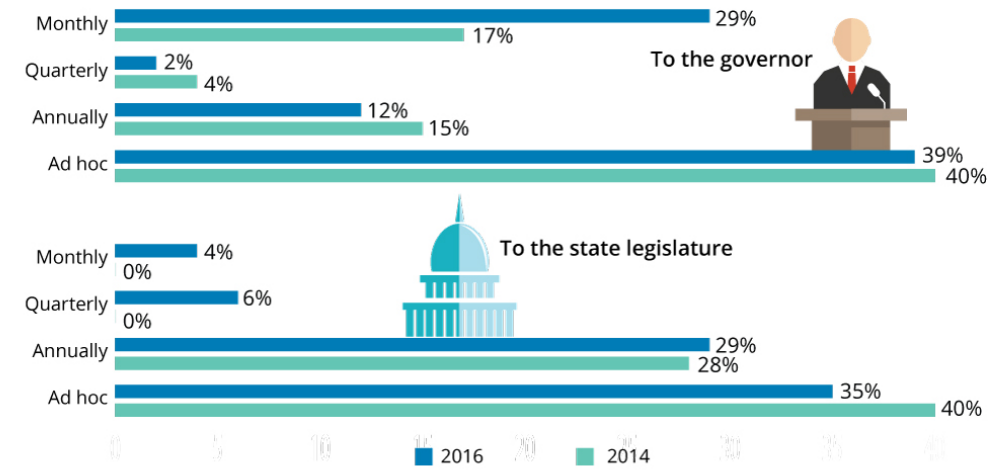
Figure 1. How often is the topic of cybersecurity presented or discussed at your agency/office executive leadership meetings?



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies. Graphic: Deloitte University Press | DUPress.com

Governors are receiving more frequent briefings on cybersecurity. Nearly a third (29 percent) of CISOs provide their governors with monthly reports on cybersecurity, compared with only 17 percent in 2014 (figure 2). However, this level of communication has not extended to state legislatures. Nearly a third of respondents say that they never communicate with their legislatures, unchanged from 2014. This is an important consideration, given the legislature's role in appropriating funds.

Figure 2. To what extent are you required to provide reports on cybersecurity status or posture of the enterprise to the following positions?



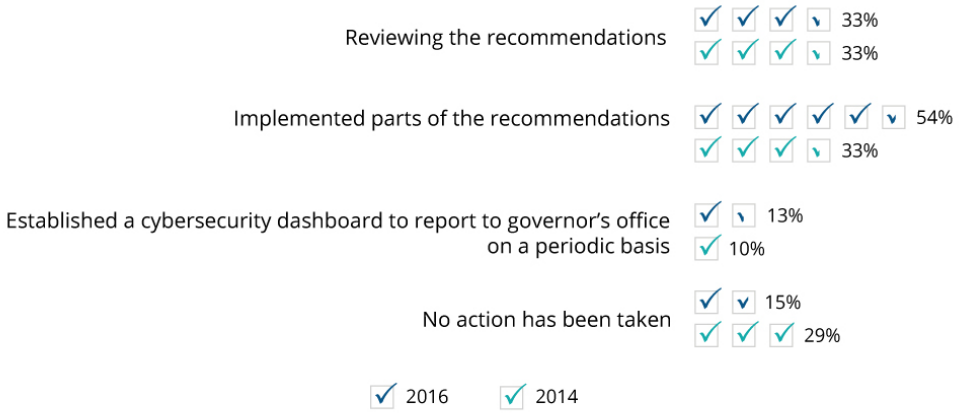
Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies. Graphic: Deloitte University Press | DUPress.com

Despite increased executive-level awareness of cybersecurity, there

remains a “confidence gap” in terms of how well CISOs versus state officials think security threats can be handled by their states. For instance, two-thirds (66 percent) of state officials say they are very or extremely confident that adequate measures are in place to protect information assets from externally originating cyber threats, compared with only a quarter (27 percent) of CISOs. These findings, which are similar to those from our 2014 study, indicate that CISOs may need to take a different approach when communicating the severity of cyber threats to state officials.

States are also starting to act and make progress in areas visible to governors. Since the NGA issued its “Act and Adjust: A Call to Action for Governors for Cybersecurity” in 2013, more than half (54 percent) of respondents say that they have implemented at least some of the NGA’s recommendations, compared with only a third (33 percent) in 2014 (figure 3). In fact, governors have launched initiatives ranging from state cyber academies and public-private partnerships to dashboards and preparedness and response plans. [1]

Figure 3. How do you characterize your state's adoption of NGA's "Act and Adjust" report? (select all that apply)



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

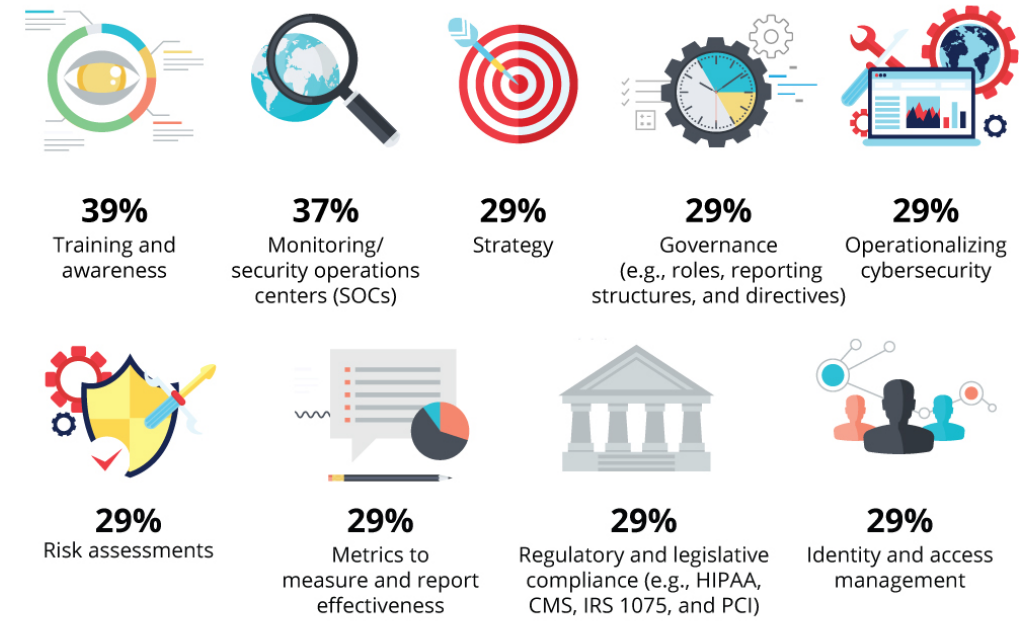
See survey analysis section for more data.

Show more

Cybersecurity is becoming part of the fabric of government operations

CISOs have begun to take a more programmatic approach to managing cyber risk and are starting to concentrate on areas that are in their control (figure 4). Only 45 percent of CISOs cited the "growing sophistication of threats" as a barrier to addressing cybersecurity challenges, down from 61 percent in 2014. CISOs are focusing on areas where they can take proactive steps to better manage risks. Some of the top areas CISOs say are within their purview include audit logs and security event monitoring, strategy and planning, and vulnerability management (figure 5).

Figure 4. Top cybersecurity initiatives for 2016



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 5. Top CISO functions

The survey respondents indicated that the top five functions within the scope of the CISO included:

*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

The CISO role itself is now a well-established position in state government. For the first time, all respondents report having an enterprise-level CISO position, an indication that states consider protecting information assets—including citizen data—from cyber threats to be an important government responsibility. CISOs' responsibilities and top priorities have remained consistent over the past two years, a sign that the role is solidifying. This conclusion is

supported by the fact that some 50 percent (24 individuals) are new to the role—yet they say their responsibilities are the same as those who have held their position for several years.

In terms of priorities, three initiatives that made the top five—training and awareness (39 percent), monitoring and SOCs (37 percent), and strategy (29 percent)—were also among the top five in 2014 (figure 4).

The mechanisms by which CISOs' authority over other organizational entities is established have not changed significantly since 2014. In addition, alignment of cybersecurity initiatives with business initiatives has increased, with 29 percent of respondents reporting appropriate alignment, versus only 14 percent in 2014. However, we continue to see CISOs have challenges in making progress on enterprise-wide initiatives in a largely federated model of governance with the agencies. For example, our results show challenges in operationalizing state-wide identity and access management (IAM) implementations. To overcome these challenges and help close the confidence gap that we continue to see, more will need to be done to elevate the authority and influence of the CISO role. CISOs need to improve communications around risks and metrics to better inform agency business executives and help promote their agendas.

See survey analysis section for more data.

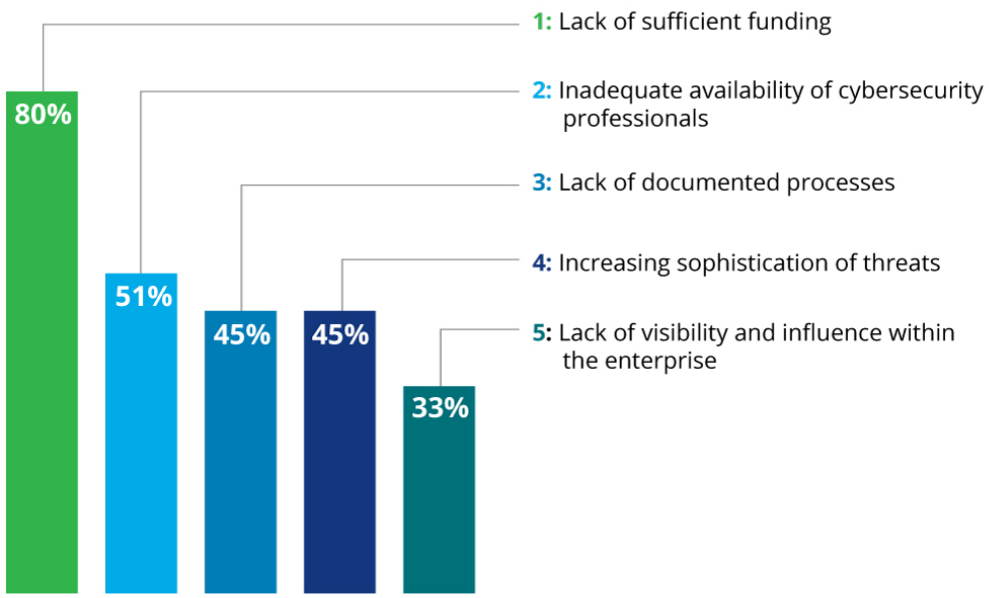
Show more

A formal strategy can lead to more resources

Even as CISOs better define their roles and become an integral part of state government, they continue to face challenges, particularly in securing the resources they need to combat ever-evolving cybersecurity threats. Four-fifths (80 percent) of respondents say inadequate funding is one of the top barriers to effectively address cybersecurity threats, while more than half (51 percent) cite inadequate availability of cybersecurity professionals (figure 6).

Figure 6. Top five barriers in addressing cybersecurity challenges

Funding still remains at the top of the list, with cybersecurity professionals next in line.



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Survey evidence suggests that when CISOs develop and document strategies—and get those strategies approved—they can command greater budgets and attract or build staff with the necessary competencies. A direct correlation can be seen between having an established strategy and obtaining more full-time equivalents (FTEs) dedicated to cybersecurity, as well as year-over-year budget

increases (figure 7). For example, 11 out of 33 states that have an approved strategy also reported they have more than 15 FTEs dedicated to cybersecurity, and 16 out of 33 states with an approved strategy reported they also had an increase in budget. An approved and proactively communicated strategy can also help CISOs overcome another barrier: "lack of visibility and influence in the enterprise," an ongoing challenge in the largely federated governance model in state government.

Figure 7. Intersection of approved strategy and resources

	More than 15 dedicated FTEs for cybersecurity	Staff has required competencies	Increase in budget	Cyber budget more than 2% of IT budget	Alignment of cyber and business programs
Approved strategy (33 states)	11 (33%)	16 (48%)	16 (48%)	10 (30%)	12 (36%)
No approved strategy (16 states)	1 (6%)	3 (19%)	5 (31%)	0 (0%)	2 (12%)

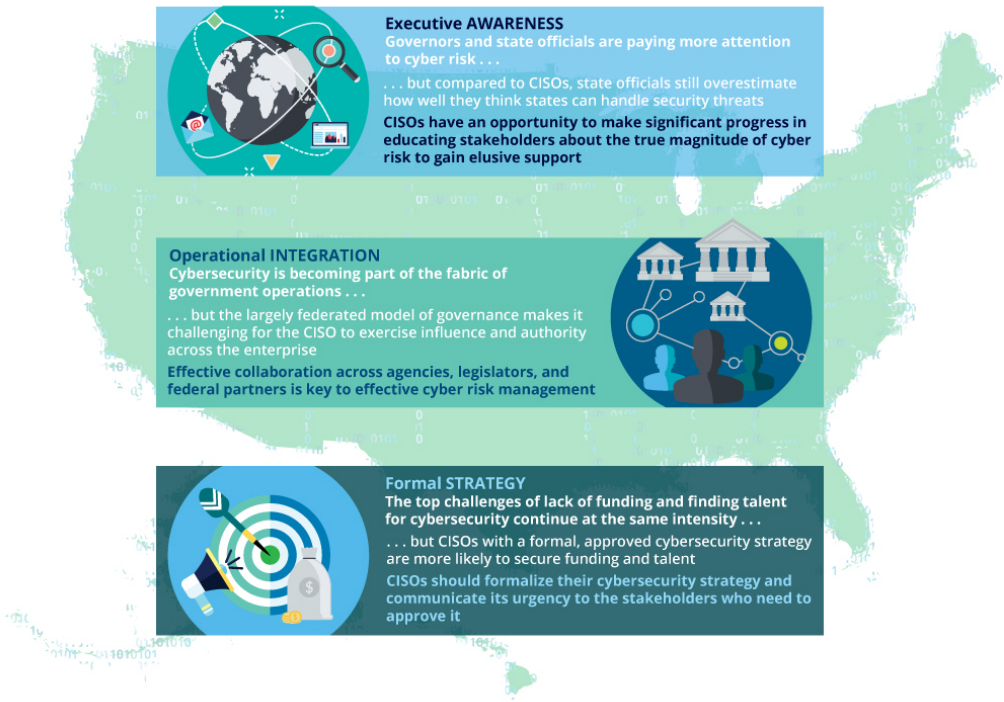
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

See survey analysis section for more data.

Show more

Key takeaways overview



Survey data analysis

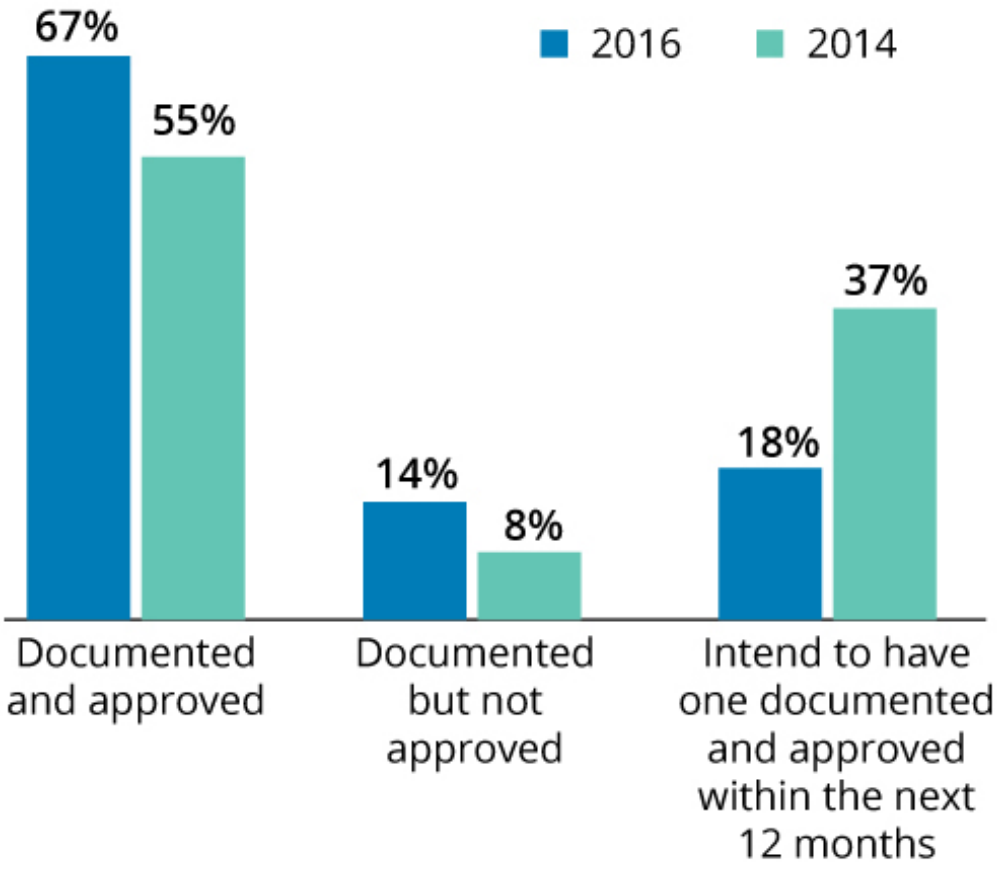
In the following section, we take a detailed look at the survey findings.

STRATEGY AND GOVERNANCE

Strategy is central to driving states' cybersecurity direction, which makes it especially important for CISOs to push for approval of their strategies. This year's survey shows that more CISOs are making progress in this regard: Two-thirds (67 percent) had cybersecurity strategies that were both documented and approved, compared with 55 percent in 2014 (figure 8). From a governance perspective, most states' security functions use a largely federated model of governance, which makes it even more important for CISOs to be effective in influencing agency business and technology stakeholders

Figure 8. States' progress in maintaining cybersecurity strategy

States are making progress in getting their strategy approved. A third of the states continue to work on getting their strategy approved.



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

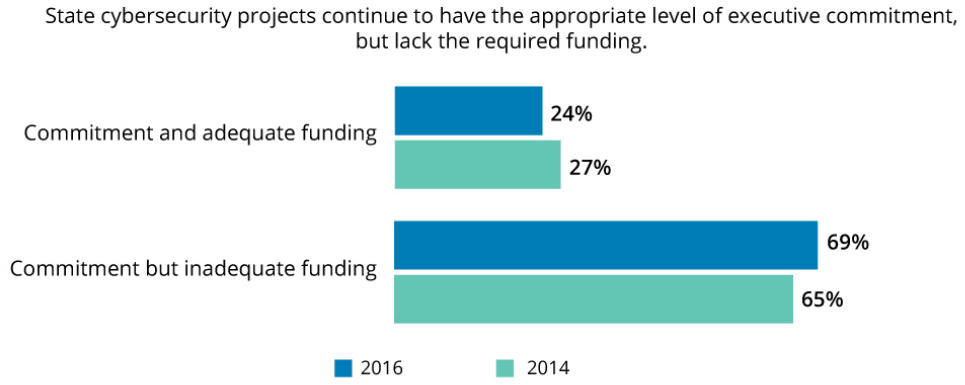
Graphic: Deloitte University Press | DUPress.com

and getting their buy-in for the strategy.

Strategies continue to involve both lines of business and technology decision makers; however, significant confidence gaps continue from the 2014 study, signifying that improvements need to be made in defining the priorities, risks, and strategies in place. A disconnect can also be seen between senior-level commitment and adequate funding (figure 9).

Collaboration across state lines and with federal agencies is also part of respondents' strategies, and it is an important means of sharing practices for addressing cybersecurity challenges (figure 10). This year, almost all respondents say that they are collaborating with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the United States Department of Homeland Security (DHS) fusion centers.

Figure 9. Senior executive support (governor's office, agency secretary, or CIO) for security projects to effectively address regulatory or legal requirements

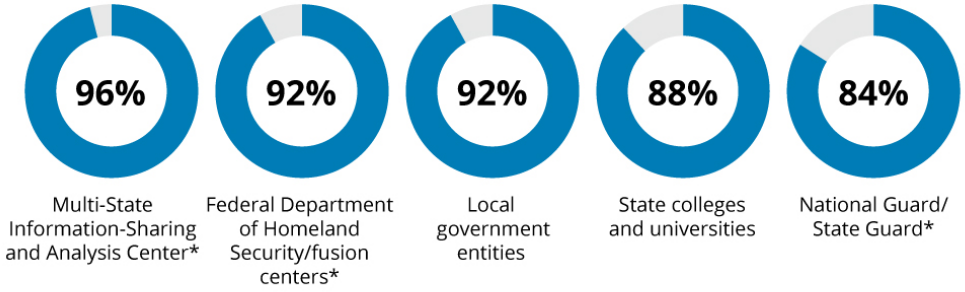


Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 10. Collaboration trends as part of the states' cybersecurity program

Collaboration is becoming central to state government strategy. Increased collaboration is an area to watch as states establish their security operations centers.



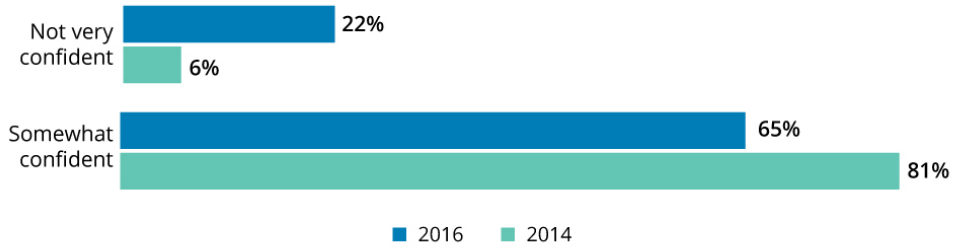
*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

CISOs are expressing a growing concern about the security practices of third parties, including those of contractors, service providers, and business partners. Nearly a quarter (22 percent) of CISOs say they are not very confident in this regard (figure 11). CISOs indicate that addressing cybersecurity in the contract is their leading option for managing the cybersecurity practices of third-party organizations (figure 12).

Figure 11. CISOs' confidence levels in cybersecurity practices followed by third parties (contractors, service providers, business partners)

CISOs' confidence level in third-party security management practices continues to be a struggle.



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 12. States' leading methods to manage adequacy of third-party (contractors, service providers, business partners, cybersecurity practices)

Ways to manage the adequacy of third-party cybersecurity practices (top five)	2016
Address cybersecurity issues in the contract	84%
Sign confidentiality and/or non-disclosure agreements	80%
Impose enterprise's cybersecurity policy and controls on third party	71%
Where allowed, perform background verification checks on select high-risk third-party employees	61%
Monitor and control third-party access to your systems and data	61%

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

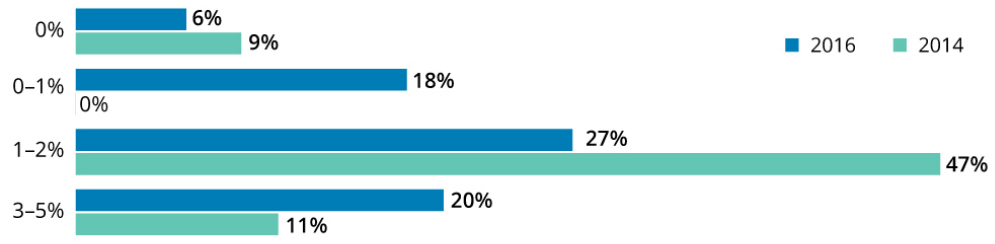
Graphic: Deloitte University Press | DUPress.com

BUDGET AND FUNDING

Lack of sufficient funding remained the most significant challenge for CISOs in 2016. The majority of respondents continue to indicate that their cybersecurity budgets were only between 0–2 percent of their state's overall IT budget (figure 13). The results did show an increase over 2014 in the 3–5 percent range of the state's overall IT budget. From a year-over-year budget perspective, 33 percent of respondents note that their budgets have remained the same (figure 14). Of the 43 percent of respondents with an increase, most of them noted increases only in the 1–5 percent range. In contrast, the federal cybersecurity budget has seen an increase of 35 percent over the 2016-enacted level. [2]

Figure 13. Percentage of state's cybersecurity allocation as part of the overall IT budget

Funding continues to be a major challenge for state CISOs. Survey results show a positive increase in the 3–5 percent range compared to 2014.

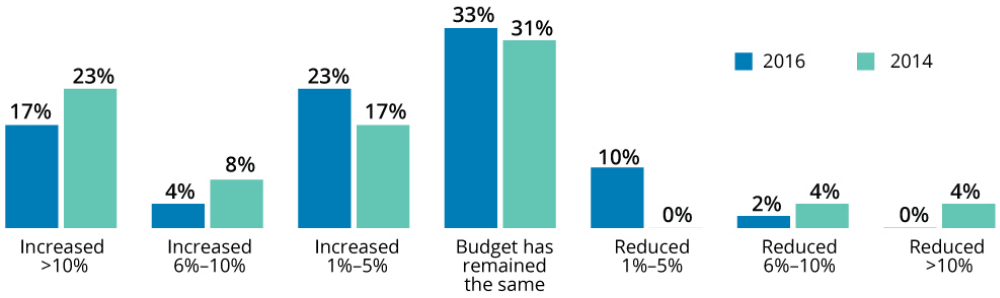


Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 14. Year-over-year trending of the state cybersecurity budget for the years 2014–2016

State cybersecurity budgets have largely remained stagnant when compared with the federal cybersecurity budget.



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Looking at the top items covered within a budget, this year's survey shows incident response as the most frequently cited (figure 15). Cybersecurity research and development and audit and certification costs moved up significantly from 2014.

Given cybersecurity's status as a national issue, states are able to tap into a range of state and federal programs and initiatives to secure additional funding (figure 16). Although limited, these are important avenues for CISOs as they build strategies to bridge the funding gap.

Figure 15. Areas covered under the cybersecurity budget

Since 2014, the top areas supported by the cybersecurity budget have changed. Logical access control, research and development, and audit/recertification have made their way into the top five.

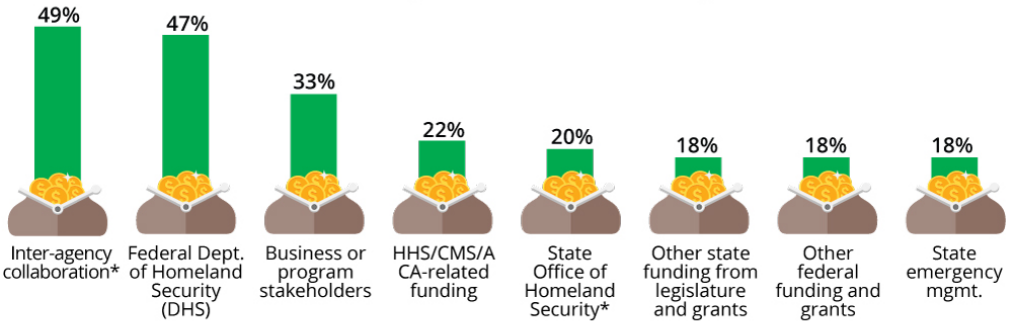
Top areas covered under the cybersecurity budget	2016	2014	Trend
Incident response	83%	69%	↑
Logical access control	79%	51%	↑
Compliance and risk management	69%	74%	↓
Cybersecurity research and development	57%	37%	↑
Audit or certification costs	48%	31%	↑
Infrastructure protection devices	40%	61%	↓
Awareness/communication costs	30%	78%	↓
Security consultants	26%	53%	↓

Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 16. Additional funding sources for cybersecurity initiatives

State CISOs have started looking at alternate sources of funding, both inside and outside their states. Inter-agency collaboration and the Department of Homeland Security are their leading sources of additional funding.



*New in 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

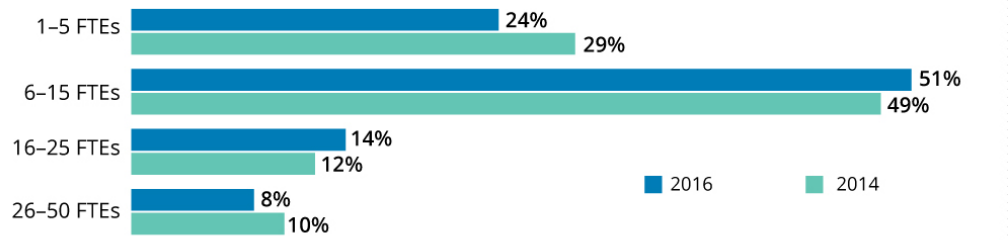
TALENT

In 2016, the cybersecurity talent crisis continues. Overall, the size of state cybersecurity staff moved up slightly, consistent with budgets (figure 17)—but not to the levels seen in the private sector or at federal agencies, which may have well over 100 FTEs handling cybersecurity. CISOs cite the inadequate availability of cybersecurity professionals as one of their biggest challenges, second only to

obtaining sufficient funding, and note salary and competition with the private sector as the top factors negatively impacting their workforce strategies (figure 18).

Figure 17. Dedicated cybersecurity professionals employed by the state's enterprise security office

The majority of states have enterprise cybersecurity teams of between 6 and 15 full-time equivalents (FTEs). Overall team size continues to show a small increase year over year.



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

Graphic: Deloitte University Press | DUPress.com

Figure 18. Top three human resources factors that negatively impact the CISO's ability to develop, support, and maintain cybersecurity workforce

State CISOs continue to identify inadequate availability of cybersecurity talent as a top barrier. The ability to attract and retain cybersecurity professionals is impacted by pay grade structures as well as by competition from the federal government and the private sector.

*New in 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

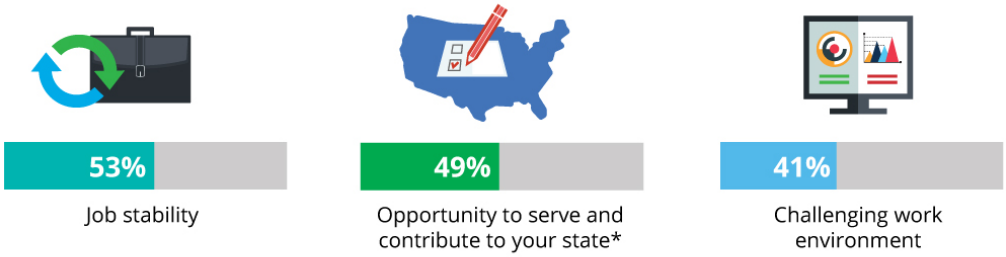
For many CISOs, their challenges are exacerbated by underfunded pension plans and budget constraints that have forced states to change retirement plans for those now entering the workforce. Attractive benefit plans, historically one of the "carrots" of a state government career, are no longer a given, and retirement packages are being restructured to more closely resemble those found in the private sector. [3] In addition, private sector salaries for information

security professionals have risen dramatically in recent years, making state government less competitive on the compensation side.

CISOs are therefore looking for other ways to win the hearts and minds of prospective employees. While more than half say that job stability is one of the top three ways to attract and retain cybersecurity talent, nearly as many point to the opportunity to serve as an important factor as well (figure 19). Promoting the potential to "give back" may be an especially effective way to attract Millennial talent, and should be built into talent acquisition plans.

Figure 19. Top three factors that CISOs employ to attract and retain cybersecurity talent

State CISOs are still grappling with the cybersecurity talent gap. Job stability, the opportunity to serve, and a challenging work environment are the top factors for attracting and retaining talent.



*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

The majority of states (56 percent) see a gap in required competencies (figure 20). To close the cybersecurity competency gap, states are using a range of strategies, including providing training, enlisting outside specialists, and outsourcing certain functional areas (figure 21). Training and awareness, the top initiative reported by states in 2016, has improved since 2014, with more respondents saying that they train a broad range of employees,

from systems administrators and programmers to executives and those handling sensitive information (figure 22).

Figure 20. State internal cybersecurity professional competencies (i.e., knowledge, skills, and behaviors) to handle existing and foreseeable cybersecurity requirements

The majority of states say their staff have gaps in cybersecurity competencies. Training, outsourcing, and staff augmentation are the leading ways that CISOs bridge the talent gap.

Source: 2016 Deloitte-NASCIO Cybersecurity Study. Graphic: Deloitte University Press | DUPress.com

Figure 21. Top outsourced cybersecurity functions

States' leading outsourced functions continue to focus on threat management services.

Outsourced functions (top five)	2016	2014
Cyber threat risk assessments	54%	37%
Forensics/legal support	44%	39%
Cyber threat management and monitoring services	35%	37%
Vulnerability management	27%	18%
Audit log analysis and reports	23%	18%

Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies. Graphic: Deloitte University Press | DUPress.com

Figure 22. Cybersecurity training trends for employees based on job role and function

States have made strides in increasing the breadth of security awareness training.

Provide required training to	Change from 2014 to 2016
Executives	↑
People handling sensitive information	↑
IT application developers and programmers	↑
System administrators	↑
IT infrastructure	↑
Business and program stakeholders	↑
General state workforce	↑
Third-party workforce (vendors, contractors, consultants, business partners)	↓

Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies. Graphic: Deloitte University Press | DUPress.com

EMERGING TRENDS

Figure 23. Top five barriers to an enterprise IAM approach

Barriers	2016
Complexity of integrating with legacy systems	67%
Competing or higher-priority initiatives*	57%
Decentralized environment of state	47%
Cost of implementation	39%
Inadequate funding to support enterprise deployment*	31%

*New in 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Identity and access management (IAM)

More states in 2016 (47 percent) than in 2014 (33 percent) have an enterprise IAM solution that covers some or all of the agencies under the governor's jurisdiction. However, CISOs continue to face the same barriers to implementing enterprise IAM solutions, including the complexity of integrating with legacy systems, cost, competing or higher-priority initiatives, and the states' decentralized IT environment (figure 23). Similar to 2014, CISOs are focusing on implementation of multifactor authentication, federated IAM, and privileged identity management solutions. Cloud-based IAM solutions and citizen identity proofing solutions follow closely as leading initiatives (figure 24).

Cyberthreats

Figure 24. States' current IAM initiatives

IAM initiatives	2016
Multifactor authentication	77%
Federated IAM for agency and third party*	48%
Privileged identity management solution	37%
Cloud-based IAM solution	27%
Citizen identity proofing solution*	15%

*New in 2016

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

CISOs view threats targeted at employees—including phishing, pharming, social engineering, and ransomware—as likely to be the most prevalent in the coming year (figure 25). This is a change from 2014, when attacks exploiting various vulnerabilities and foreign-sponsored espionage topped the list. CISOs continue to be "somewhat confident" in their states' abilities to protect against cyberthreats (figure 26). They appear most confident in their ability to protect against internal threats and least confident when it comes to threats originating from emerging technologies.

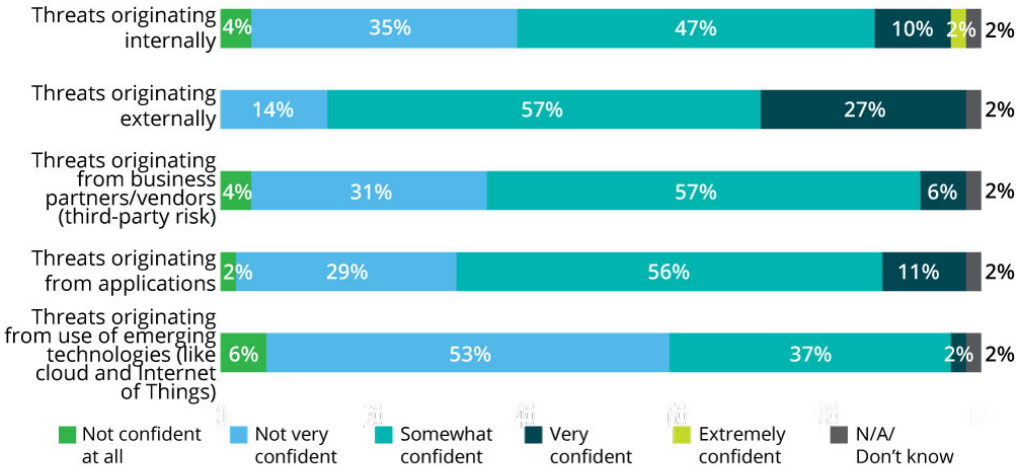
Figure 25. Prevalence of cyberthreats across state governments

	Somewhat higher threat	Very high threat
Phishing, pharming, and other related variants	35%	47%
Social engineering	31%	42%
Ransomware	43%	29%
Increasing sophistication and proliferation of threats (e.g., viruses, worms, and malware)	51%	14%
Exploits of vulnerabilities from unsecured code	45%	8%

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Figure 26. CISOs' confidence levels in protecting their state's information assets from cyber threats



Source: 2016 Deloitte-NASCIO Cybersecurity Study. Graphic: Deloitte University Press | DUPress.com

Assessments

The majority of the states continue to perform ad-hoc assessments to evaluate their cybersecurity posture (figure 27). More frequent assessments could provide a better baseline for determining the effectiveness of cybersecurity controls.

Figure 27. Frequency of cybersecurity assessments

	Monthly	Quarterly	Semi-annually	Annually	Ad hoc
Security code review	6%	2%	0%	8%	63%
Security risk assessment	0%	2%	2%	33%	54%
Internal penetration testing	17%	4%	4%	15%	52%
Application security vulnerability testing	13%	13%	2%	17%	50%
Cyber threat intelligence analytics	35%	2%	0%	2%	48%
External penetration testing	13%	2%	0%	29%	46%
Penetration testing conducted by third party	4%	6%	0%	33%	46%
Privacy impact assessment	0%	0%	2%	13%	44%
Cyber incident simulation or wargaming (to prepare for a cyberattack) and business continuity exercises	2%	6%	10%	33%	33%
Annual disaster recovery exercises and tests	2%	0%	10%	50%	29%
Security events monitoring/ security operations center	60%	0%	0%	6%	23%

Source: 2016 Deloitte-NASCIO Cybersecurity Study. Graphic: Deloitte University Press | DUPress.com

Cybersecurity technology adoption

More states have adopted traditional cybersecurity solutions, such as firewalls and antivirus software (figure 28). CISOs indicate that security compliance, network behavior analysis, data protection, and IAM solutions lead the next wave of enterprise adoption.

Figure 28. Top emerging technologies

		Plan to fully deploy or pilot within the next 12 months	Currently piloting	Fully deployed
Leading technologies being deployed or piloted in the next 12 months	Security compliance tools	**52%**	6%	21%
	Multifactor authentication	**49%**	14%	22%
	Federated identity management	**38%**	19%	19%
Leading technologies that are currently being piloted	Biometric technologies for user authentication	8%	**25%**	4%
	Network behavior analysis	29%	**21%**	27%
	Data loss prevention technology	37%	**20%**	25%
Leading technologies that are fully deployed	Firewalls	2%	0%	**96%**
	Antivirus	4%	0%	**92%**
	Spam filtering solutions	2%	2%	**90%**

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Cyber legislation

Several state legislatures have been active in providing guidance to CISOs regarding implementation of cybersecurity measures—particularly in the areas of data breach reporting and notification. However, most states do not have established cybersecurity legislation in place (figure 29). More than a quarter (29 percent) of states have reported an increase in funding from legislation and grant sources.

Figure 29. Provisions of states' cyber legislation/statutes

	Established and funded	Established and not funded	In progress	Not in place
Cybersecurity incident/data breach reporting and handling	43%	21%	4%	32%
Data breach notification	41%	35%	2%	23%
Role and authority of the enterprise CISO or equivalent	40%	4%	2%	54%
Continuity of government/continuity of operations	35%	13%	4%	48%
Cybersecurity awareness	31%	4%	2%	63%
Data privacy provisions: authority and purpose; collection, storage, use, and sharing limitations	27%	21%	2%	50%
State-level cybersecurity program and framework for enterprise risk management	27%	17%	8%	48%
Cybersecurity budget allocation and review	26%	0%	4%	70%
Cyber threat information-sharing program between state agencies, law enforcement, and private entities	21%	10%	6%	63%
Public-private partnerships or council to support the state's cybersecurity programs	13%	2%	4%	81%
Cybersecurity workforce development and training	11%	4%	4%	81%
Cybersecurity legislative council or equivalent to do a periodic review, steer the state's cybersecurity posture, and allocate funding	11%	10%	6%	73%
Role and authority of the enterprise chief privacy officer (CPO) or equivalent	6%	2%	2%	90%

Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

Moving forward

In the past two years, CISOs have moved their states forward in the fight against cyber risk. But the threat environment is so complex and evolving that many challenges remain. States faced with a myriad of priorities and ongoing resource constraints may be hard-pressed to allocate sufficient funding to cybersecurity initiatives. Competition for top talent can make it difficult to attract the professionals needed to effectively combat constantly evolving threats.

But CISOs do have one thing in their favor: State executives, including governors, are starting to pay more attention to the issue of cybersecurity. Those who are able to harness this attention have an opportunity to garner more resources and support for their initiatives. In order to make further progress, CISOs should think about the following:

- **Strategy** : Document and formalize the cybersecurity strategy. Going through the process of socializing the strategy with a broad range of stakeholders has a number of benefits. It ensures input from each of these parties, improving the overall strategy as a result. It strengthens collaborative relationships with other state agencies and departments. It raises awareness of cybersecurity issues. And finally, as our results have shown, it increases the chances of garnering more funding.
- **Funding** : Work with stakeholders to make cybersecurity a significant line item on state IT and business initiative budgets. For most states, cybersecurity is less than 2 percent of the overall IT budget. Cybersecurity is a business risk to state government, and funding should be commensurate with the risk.
- **Communications** : Use metrics and numbers to tell a compelling story about cyber risk. The fact that state officials are significantly more confident than CISOs about their states' ability to protect against cyber risk indicates that the right message still may not be getting across. State officials' lack of insight into the

true business risks of cyberthreats could even affect funding. It is important for CISOs to step up the frequency of their communications—especially with agency business executives and legislators—and to communicate the risks more effectively.

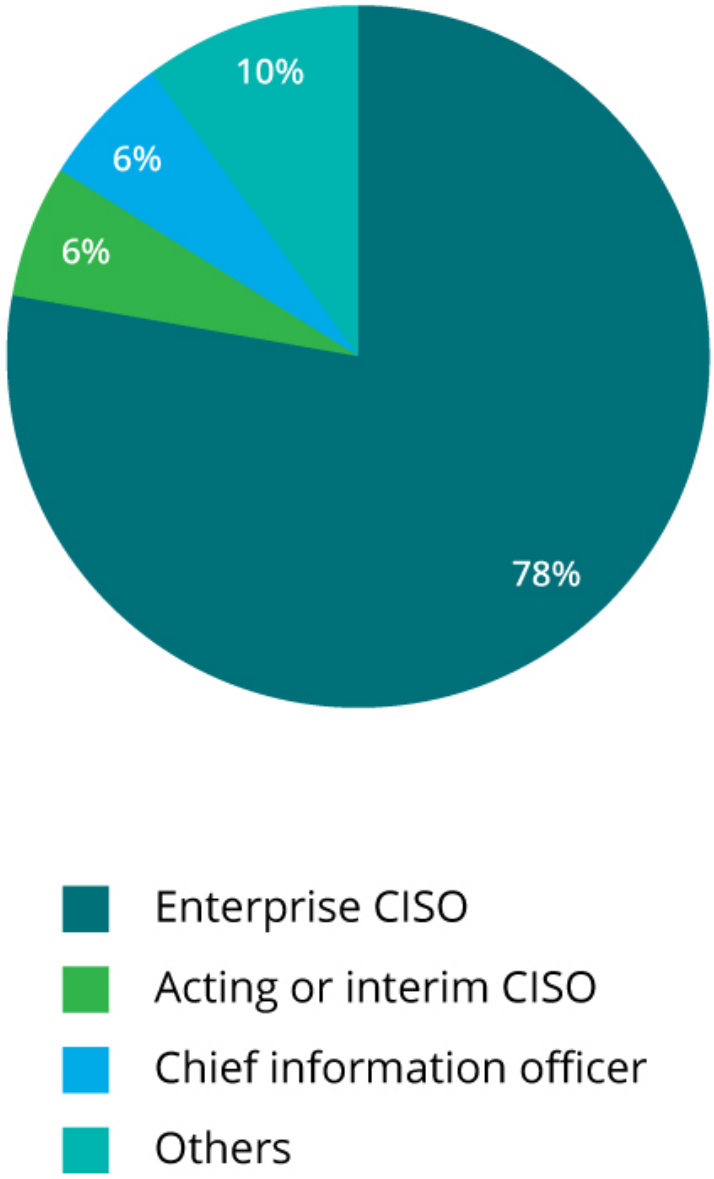
- **Talent** : Promote the right benefits, modernize your workplace culture, and better define required skills to attract the right talent. The nature of what states have to offer workers has changed—which can be an advantage if positioned correctly. Millennials are not necessarily attracted by the promise of a secure retirement—something fewer states today are able to offer. Many of them find the prospect of "giving back" to be a more compelling reason to gravitate toward an employer. This, along with a rich training and development program, can serve as the basis for a campaign to recruit Millennial talent.

States should consider these components as they better define their strategy and look to create a higher level of awareness. These approaches can help CISOs continue their progress in combating cyber risks.

Appendix: Survey methodology

THE 2016 DELOITTE-NASCIO

Figure 30. CISO survey respondent designation



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

CYBERSECURITY STUDY USES SURVEY RESPONSES FROM:

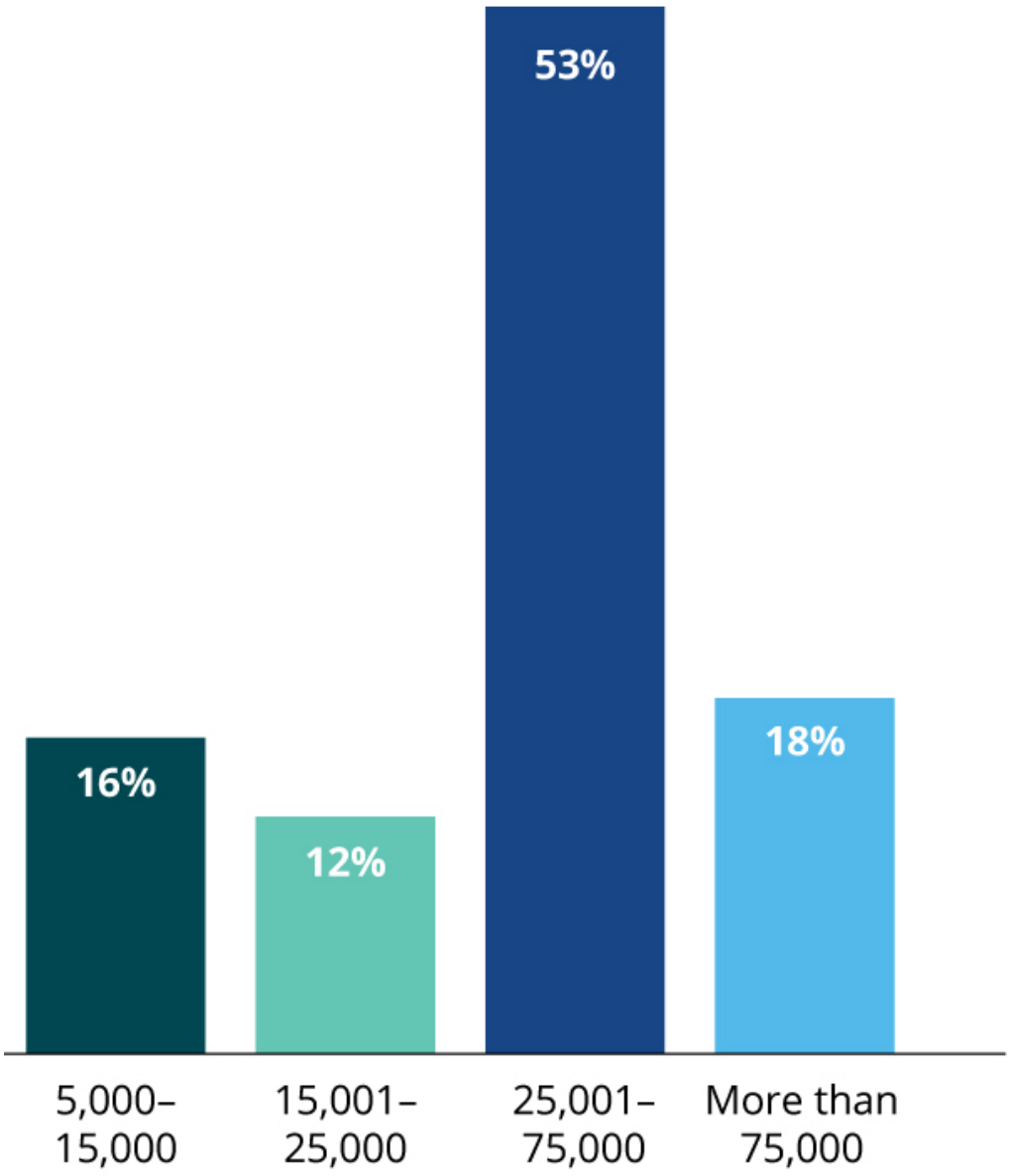
- US state enterprise-level CISOs, with additional input from state agency CISOs and security staff members

- US state (business) officials, using a survey designed to help characterize how the state government enterprise views, formulates, implements, and maintains its security programs

CISO PROFILE

CISO participants answered 59 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs. Participation was high: Responses were received from 49

Figure 31. Number of government employees in your state (excluding higher education employees)



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

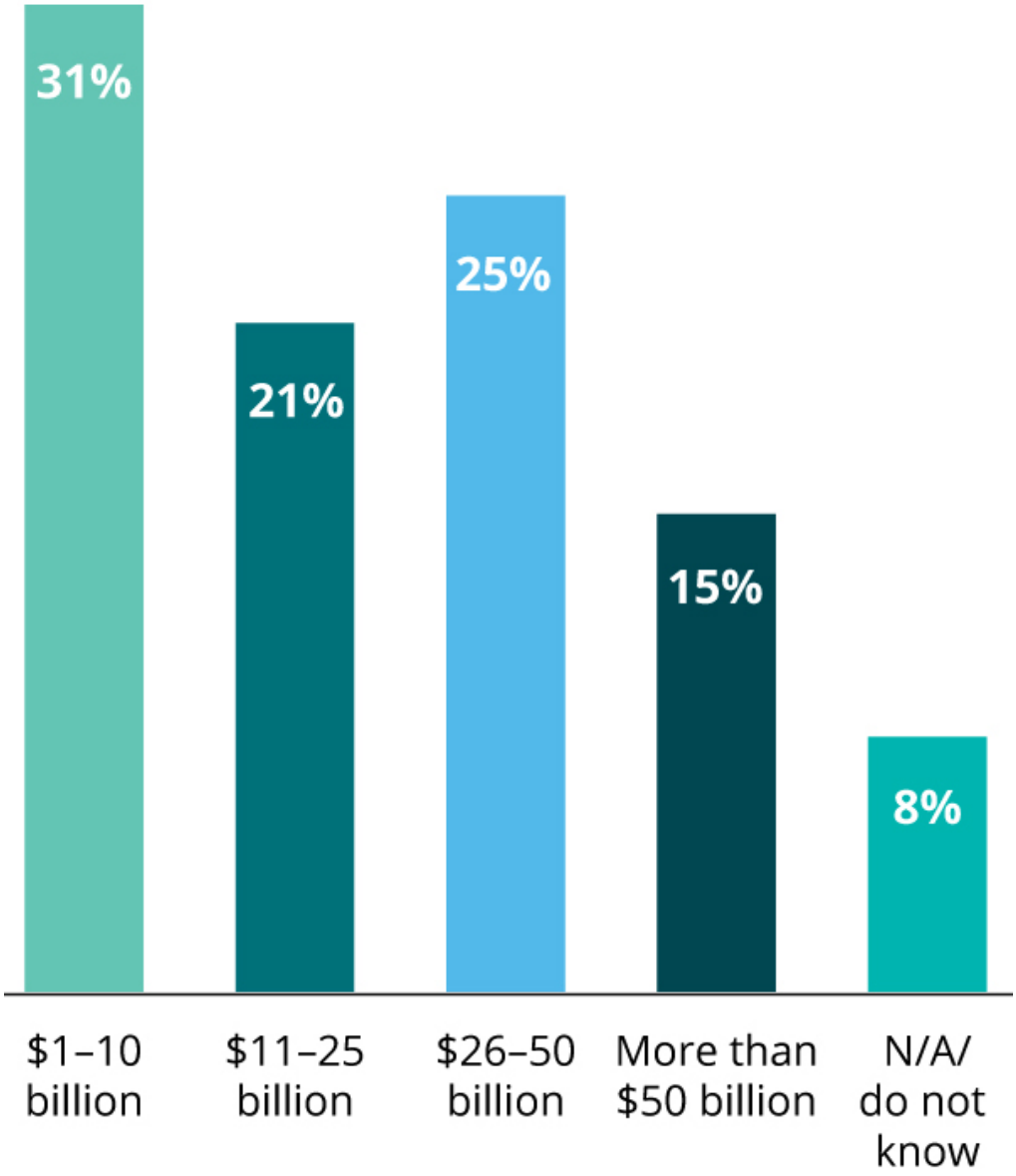
states and territories. Figures 30–32 illustrate the CISO participants' demographic profile.

STATE OFFICIAL PROFILE

Ninety-six state business and elected officials answered 15 questions, providing valuable insight into state business stakeholder perspectives. The participant affiliations included the following associations:

- National Association of State Budget Officers (NASBO)
- National Association of State Auditors, Comptrollers, and Treasurers (NASACT)
- National Association of Attorneys General (NAAG)
- National Association of Secretaries of State (NASS)
- National Association of State Personnel Executives (NASPE)
- National Association of State Chief Administrators (NASCA)
- National Association of State Procurement Officials (NASPO)
- National Association of Medicaid Directors (NAMD)
- National Emergency Management Association (NEMA)
- Federation of Tax Administrators (FTA)
- Governors Homeland Security Advisors Council (GHSAC)
- International Association of Chiefs of Police (IACP)—Division of State and Provincial Police (S&P)

Figure 32. Approximate annual budget of the respondent states (USD)



Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

The two surveys provided an opportunity for survey respondents to add additional comments when they wanted to further explain "N/A" or "other" responses. A number of participants provided such comments, offering further insight into the analysis.

HOW DELOITTE AND NASCIO DESIGNED, IMPLEMENTED, AND EVALUATED THE SURVEY

Deloitte and NASCIO collaborated to produce the 2016 Deloitte-NASCIO Cybersecurity Study. Working with NASCIO and several

Deloitte Insights: New name, same commitment to delivering insights that matter. Learn more ×

questionnaire to probe key aspects of information security within state government. A CISO survey review team, consisting of the members of the NASCIO Cybersecurity Committee, evaluated the survey questions and assisted in further refining the survey questions.

In most cases, respondents completed the surveys using a secure online tool. Respondents were asked to answer questions to the best of their knowledge and had the option to skip a question if they did not feel comfortable answering it. Each participant's response is confidential, and any identifying information was deleted after the preparation of the survey reports.

The data collection and analysis was conducted by DeloitteDEX, Deloitte's proprietary survey and benchmarking service. Results of the survey have been analyzed according to industry-leading practices and reviewed by senior members of Deloitte's Cyber Risk Services practice, the Deloitte Center for Government Insights, and Deloitte's Technology and Human Capital practices. In some cases, in order to identify trends or unique themes, data were also compared to prior surveys and additional research. Results on some charts may not total 100 percent based on answer choices such as

“not applicable,” “do not know,” or “other.”

Due to the volume of questions, and for better readability, this document reports only the data points deemed to be most important at the aggregate level. A companion report, including all questions and benchmarked responses, has been provided individually to the state CISO survey respondents.

Credits

Written By: **Doug Robinson** < *https://dupress.deloitte.com/dup-us-en/authors/r/doug-robinson.html*> , **Srini Subramanian** < *https://dupress.deloitte.com/dup-us-en/authors/s/srini-subramanian.html*>

Acknowledgements

CONTRIBUTORS

We thank the NASCIO and Deloitte professionals who helped to develop the survey and execute, analyze, and create the report.

NASCIO

Doug Robinson, executive director

Meredith Ward, senior policy analyst

Members of the state CISO survey review team

Maria Thompson, State of North Carolina

Agnes Kirk, State of Washington

Marcos Vieyra, State of South Carolina

Erik Avakian, Commonwealth of Pennsylvania

Jim Edman, State of South Dakota

Elayne Starkey, State of Delaware

Deborah Blythe, State of Colorado

Deloitte subject matter specialist contributors

Bharane Balasubramanian, Deloitte & Touche LLP

Bill Eggers, Deloitte Services LP

Art Stephens, Deloitte Consulting LLP

Srini Subramanian, Deloitte & Touche LLP

John O'Leary, Deloitte Services LP

Peter Viechnicki, Deloitte Services LP

Mike Wyatt, Deloitte & Touche LLP

Deloitte survey team, data analysis, and benchmarks

Balaji Kannan, Deloitte & Touche LLP

Pankaj Kamleshkumar, Deloitte Support Services India Private Limited

Marketing

Annette Evans, Deloitte Services LP

Topics in this article

Cyber risk < *https://dupress.deloitte.com/dup-us-en/tags/cyber-risk.html*> , **State Government** < *https://dupress.deloitte.com/dup-us-en/tags/state-government.html*> , **Public Sector** < *https://dupress.deloitte.com/dup-us-en/tags/public-sector.html*> , **Government** < *https://dupress.deloitte.com/dup-us-en/tags/government.html*>

Endnotes

1 National Governors Association, "Resource center for state cybersecurity," **http://www.nga.org/cms/statecyber** <http://www.nga.org/cms/statecyber> , accessed September 10, 2016.

2 ITDashboard.gov, **https://itdashboard.gov/** <https://itdashboard.gov/> ; The White House, *President's IT budget for FY 2017,* **https://www.whitehouse.gov/sites/default/files/omb/egov/documents/fy17_agency_submission_topline.pdf** <https://www.whitehouse.gov/sites/default/files/omb/egov/documents/fy17_agency_submission_topline.pdf> .

3 Steven Greenhouse, "Pension funds strained, states look at 401(k) plans," New York Times, February 28, 2011, **http://www.nytimes.com/2011/03/01/business/01pension.html?_r=0** <http://www.nytimes.com/2011/03/01/business/01pension.html?_r=0> .

© 2017. See Terms of Use <https://www2.deloitte.com/us/en/legal/terms-of-use.html> for more information.

Global Cyber Security Capacity Centre

Cyber Security Awareness Campaigns
"Why do they fail to change behavior?"
Draft Working Paper

July 2014

Global Cyber Security Capacity Centre

Global Cyber Security Capacity Centre: Draft Working Paper

Cyber Security Awareness Campaigns Why do they fail to change behaviour?

Dr. Maria Bada
Global Cyber Security Capacity Centre,
University of Oxford

Professor Angela Sasse
Department of Computer Science
Science of Cyber Security Research Institute
University College London

July 2014

Contents

Abstract 4

1 Introduction 5

1.1 Scope and purpose 5

1.2 Structure of the paper 5

1.3 Audience 6

2 Theoretical Background 7

2.1. Theory of reasoned action 7

2.2. Theory of planned behaviour 7

2.3. Protection motivation theory 8

2.4. Self-efficacy 8

2.5. Expected utility hypothesis 8

3. Information Security Awareness Campaigns 10

4. Persuasion Techniques 12

4.1. Behaviour Change 12

4.2. Influence Strategies 12

4.3. Factors influencing change 14

4.3.1. Personal Factors 14

4.3.1.1. Security Fatigue 15

4.3.2. Social Factors 15

4.3.3. Environmental Factors 15

4.4. Fear 16

4.4.1. Fear as a persuasion approach 16

4.5. Control 16

5. Culture 18

5.1. Culture and Risk perception 19

6. Rewards and Punishments 20

7. Media-Framed Messages 21

8. Essential Components for a Campaign 22

9. Factors which lead to a Campaign's failure 23

10. Case Studies 24

10.1. Cyber Security Awareness Campaigns in U.K. 24

10.2. Cyber Security Awareness Campaigns in Australia 29

10.3. Cyber Security Awareness Campaigns in Canada 31

10.4. Cyber Security Awareness Campaigns in Africa 31

11. Conclusions 33

References 35

Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

Dr. Maria Bada
Global Cyber Security Capacity Centre, University of Oxford, maria.bada@cs.ox.ac.uk

Professor Angela Sasse
Department of Computer Science, Science of Cyber Security Research Institute, University College London, A.Sasse@cs.ucl.ac.uk

Abstract
The present paper focuses on Security Awareness Campaigns, trying to identify factors which potentially lead to failure of these in changing the information security behaviours of consumers and employees. Past and current efforts to improve information security practices have not had the desired effort. In this paper, we explain the challenges involved in improving information security behaviours. Changing behaviour requires more than giving information about risks and correct behaviours – firstly, the people must be able to understand and apply the advice, and secondly, they must be willing to do – and the latter requires changes to attitudes and intentions. These antecedents of behaviour change are identified in several psychological models of behaviour (e.g. theory of reasoned action, theory of planned behaviour, protection motivation theory). We review the suitability of persuasion techniques, including the widely used fear appeals. Essential components for an awareness campaign as well as factors which can lead to a campaign's failure are also discussed.

In order to enact change, the current sources of influence-whether they are conscious or unconscious, personal, environmental or social, which are keeping people from enacting vital behaviours, need to be identified. Cultural differences in risk perceptions can also influence the maintenance of a particular way of life. Finally, since the vast majority of behaviours are habitual, the change from existing habits to better information security habits requires support. Finally, we present examples of existing awareness campaigns in U.K., in Australia, in Canada and Africa.

1 Introduction

1.1 Scope and purpose

Governments and commercial organizations around the globe make extensive use of information and computing (ICT) systems, and need to keep them secure. To achieve this, they deploy technical security measures, and develop policies that specify 'correct' behaviour of employees, consumers and citizens. There is ample evidence that many people do not comply with specified behaviours - some because do not know the risks or the correct behaviour, but most people who do not comply know the correct behaviour when asked.

The primary purpose of security awareness is to influence the adoption of secure behaviours. In this report, we will identify first what behaviours help to deliver information security, and to what extent they are adopted. We will then examine existing approaches to change information security behaviours through awareness campaigns - what works, and what not, and why.

The aim of this paper is to take a first step towards understanding better the reason why changing information security behaviour is such a challenge. IT requires more than simply telling people what they should and should not do: they need first of all to accept that the information is relevant, secondly understand how they ought to do, and thirdly be willing to do this, in the face of many other demands. In order to enact change, the current sources of influence- whether they are conscious or unconscious, personal, environmental or social, which are keeping people from enacting vital behaviours, need to be found. Cultural differences in risk perceptions can also influence the maintenance of a particular way of life.
Finally: even when people are willing to change, the process of learning a new behaviour needs to be supported.

We discuss components for an awareness campaign as well as factors which can lead to a campaign's failure.

1.2 Structure of the paper

Section 2 of this paper reviews existing knowledge about behaviour and behaviour change in general. Models such as the theory of reasoned action, the theory of planned behaviour, protection motivation theory, as well as the importance of self-efficacy as a personal factor are being presented.

Section 3 reviews current information security awareness campaigns and their effectiveness. In section 4, we examine persuasion techniques used in past campaigns. Many campaign designers use fear to encourage people to adopt better practices. Psychological research findings show the importance of fear in attitude and / or behavior change Influence strategies. Also factors which influence change, such as personal, social and environmental factors, are described.

In Section 5 we consider the importance of cultural differences as a factor which influences or prohibits behavioural change. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient.

Section 6, discusses rewards and punishments as a method of influencing people in order to follow a desired behaviour. Section 7, presents the importance of message framing and their persuasiveness.

Section 8, summarises the essential components for a campaign, and section 9 presents the factors which can lead to a campaign's failure.

The last part of this paper, section 10, presents examples of existing awareness campaigns in U.K., in Australia, in Canada and Africa.

1.3 Audience

This paper is written primarily for experts on awareness campaigns, influence strategists as well as experts on education and training.

2 Theoretical Background

In order to change behaviour, there has to be a change in attitudes and intentions. These antecedents of behaviour change are key indices of a person's mental readiness for action and are described in several psychological models of behaviour (e.g. theory of reasoned action, theory of planned behaviour, protection motivation theory).

2.1. Theory of reasoned action

The theory of reasoned action (Ajzen & Fishbein, 1980) proposes an internal decision mechanism in which the formation of intention of behavior is immediately preceding the same behavior and mediates between that and the impact of other variables. According to this theory, the psychological requirements of intended behavior are attitudes and perceived social norms.

Overall, the model supports a linear process in which changes in behavior and normative beliefs of an individual will ultimately affect the actual behavior. Perceived control, the sense one has that he/she can drive specific behavior has been found to affect the intention of behavior but also the real behavior.

2.2. Theory of planned behaviour

The theory of planned behaviour (TPB) was developed by Ajzen in 1988. The theory proposes a model which can measure how human actions are guided. It predicts the occurrence of a particular behaviour, provided that behaviour is intentional.

The theory was intended to explain all behaviours over which people have the ability to exert self-control. The key component to this model is behavioural intent. Behavioural intentions are influenced by the attitude about the likelihood that the behaviour will have the expected outcome and the subjective evaluation of the risks and benefits of that outcome.

The TPB states that behavioural achievement depends on both motivation (intention) and ability (behavioural control). It distinguishes between three types of beliefs - behavioural, normative, and control. The TPB is comprised of six constructs that collectively represent a person's actual control over the behaviour.

1. Attitudes - refer to the degree to which a person has a favourable or unfavourable evaluation of the behaviour of interest. It entails a consideration of the outcomes of performing the behaviour.
2. Behavioural intention - refers to the motivational factors that influence a given behaviour where the stronger the intention to perform the behaviour, the more likely the behaviour will be performed.
3. Subjective norms - refer to the belief about whether most people approve or disapprove of the behaviour. It relates to a person's beliefs about whether peers and people of importance to the person think he or she should engage in the behaviour.
4. Social norms - refer to the customary codes of behaviour in a group or people or larger cultural context. Social norms are considered normative, or standard, in a group of people.

5. Perceived power - refers to the perceived presence of factors that may facilitate or impede performance of a behaviour. Perceived power contributes to a person's perceived behavioural control over each of those factors.
6. Perceived behavioural control.

2.3. Protection motivation theory

Protection motivation theory was originally developed to explain the influence of fear invocations on attitudes and health behaviors (Rogers, 1975).
Protection motivation theory is organized around two cognitive processes: the process of threat assessment and the process of handling assessment.

Based on only one factor of protection motivation theory, vulnerability, we can say that many other factors prevent people to appreciate properly the possibilities of a result. It is important to note that the final threat assessments and handling reflections will react through measurements of intent and behavior.

2.4. Self-efficacy

According to theory of Self-efficacy (Bandura 1977), the adoption of a preventive health behavior, depends on three factors:

- the realization that the person is at risk,
- the expectation that behavior change will reduce this risk and
- the expectation that the person is capable enough to adopt preventive behavior or to refrain from risky health behavior.

It is not simply a matter of how capable is someone but how capable he/she considers to be. Bandura (1977), successfully showed that people with different levels of self-efficacy perceive the world differently. Individuals with a high sense of self-efficacy are generally of the opinion that they have absolute control over their lives. That their personal actions and decisions shape their lives. In contrast, individuals with low sense of self-efficacy feel that their lives do not depend on them.

Our beliefs about self-efficacy, affect the way we think and of course affect our emotional reactions.

2.5. Expected utility hypothesis

In economics, game theory, and decision theory the expected utility hypothesis refers to a hypothesis concerning people's preferences with regard to choices that have uncertain outcomes (gambles). This hypothesis states that if certain axioms are satisfied, the subjective value associated with a gamble by an individual is the statistical expectation of that individual's valuations of the outcomes of that gamble (Bernoulli, Daniel, 1954).
According to the expected utility approach, behavioural change can be explained because individuals perceive it as a 'useful' decision. In the presence of risky outcomes, a decision maker could use the expected value criterion as a rule of choice: higher expected value investments are simply the preferred ones. This hypothesis has proved useful to explain some popular choices

that seem to contradict the expected value criterion (which takes into account only the sizes of the pay-outs and the probabilities of occurrence), such as occur in the contexts of gambling and insurance.

3. Information Security Awareness Campaigns

There is a need to move from awareness to tangible behaviours. Governments and Organizations need to secure their information assets and systems, and develop policies that specify the expected, 'correct' behaviours for their employees. Governments encourage citizens to transact online – and dispense advice on how to do so. But there is ample evidence that major cyber events continue to occur (Kirlappos & Sasse, 2012, Kirlappos, Parkin, & Sasse, 2014). Training as conceived is not working. Caputo, et al., (2013) having spear phishing as an example showed that framing had no significant effect. The study suggested that effective embedded training must take into account not only framing and security experience but also perceived security support, information load, preferred notification method and more.

The fact is that people know the answer to awareness questions but they do not act accordingly to their real life (ISF, 2014, NIST, 2003). The Coventry, et al., report (2014, Government Office for Science, UK) proposes that it is essential for security and privacy practises to be designed into a system from the very beginning. A system difficult to use will eventually lead users to make mistakes and avoid it.

The primary purpose of security awareness is to render people amenable to change (Winkler, I. & Manke, S, 2013). Influence strategists need to identify vital behaviours, meaning behaviours which they wish to change before they start trying to change them. Equally important is identifying the crucial moments when they are most likely to fail in meeting these goals (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011).

Awareness is defined in NIST Special Publication 800-16 (Wilson and Hash, 2003) as follows: "*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.*

Questions rise on what exactly is not working and the majority of security awareness campaigns cannot secure the human element. The most recent ISF report (2014), identifies the following reasons:

1. Solutions are not aligned to business risks
2. Neither progress nor value are measured
3. Incorrect assumptions are made about people and their motivations
4. Unrealistic expectations are set
5. The correct skills are not deployed
6. Awareness is just background noise

Persuasiveness of recommendations for health, among other things, is a function of assessing the cost of the recommended behaviour - such as money, time, effort and discomfort - and the reaction efficiency, defined as the probability that compliance with the recommendation will lead to the desired goal.

Various behavioural theories consider the cost and efficiency of a reaction and have independent effects on persuasion. Among health messages, more effective are those tailored to the

individual's needs (Simons-Morton, et. Al., 1997). However, even when the design of the message is taken into account, there is a big gap between the recognition of the threat and the manifestation of the desired behaviour at regular intervals. The attempt to change a certain behaviour is much more difficult when the person is bombarded by a large number of messages about certain issues.

Naturally, an individual who is faced with so many warnings and advice, may be tempted to abandon all efforts to protect himself, and not worry about any danger (Fisher & Rost, 1986). Threatening or intimidating messages are not particularly effective, for the reason that they increase the stress of the individual to such an extent that the individual may even be repulsed or deny the existence of any problem.

An awareness and training program is crucial in that it is the vehicle for disseminating information that users, including managers, need in order to do their jobs. In the case of an IT security program, it is the vehicle to be used to communicate security requirements across the enterprise. An awareness and training program can be effective, if the material is interesting and current. Any presentation that "feels" impersonal and so general as to apply to any audience, will be filed away as just another obligatory session (NIST, Wilson and Hash, 2003).

Briefly, a persuasive message must have four characteristics: First, it needs to attract attention, secondly, it must be understood, thirdly, it must relate to a matter worthy processing and fourthly, its contents will need to be stored and recalled easily from memory.

Research findings show that it is better to present the arguments on both sides. In that case the recipient is able to autonomously decide which of the two would believe. If only convinced by the arguments in favour of a view and then opposing arguments are presented, then it is likely that the initial convictions falter and weaken.

Findings of studies on persuasion, highlighted the existence of an important phenomenon, called ''retardant effect of persuasion'', which refers to persuasion brought about the desired results after a long time later. This phenomenon occurs when the initial belief of a message is changing, and the recipient cannot remember what caused the change (Cook & Flay, 1978).

4. Persuasion Techniques

4.1. Behaviour Change

Persuasion can be defined as an "*Attempt to change attitudes or behaviors or both (without using coercion or deception)" (Fogg, 2002).* There are basically two ways of thinking about changing behaviour (Dolan, et al., MINDSPACE, 2010). The first is based on influencing what people consciously think about, rational or cognitive model. This model suggests that citizens and consumers will analyse the various pieces of information from various sources, the numerous incentives offered to them and act in their best interests. The second model of shaping behaviour focuses on the more automatic processes of judgment and influence. This shifts the focus of attention away from facts and information, and towards altering the context within which people act, the context model. The context model recognises that people are sometimes seemingly irrational and inconsistent in their choices, often because they are influenced by surrounding factors. It focuses more on 'changing behaviour without changing minds'. This route has received rather less attention from researchers and policymakers.

Three factors are particularly useful for understanding controversy around behaviour change (Dolan, et al., MINDSPACE, 2010).

1. **Who the policy affects.** Any behaviour change that will affect a group in particular is likely to require careful justification–there may be particular controversy if the behaviour concerned is seen as integral to a group's identity or culture.
2. **What type of behaviour is intended.** If the harm is seen to be more distant from the individual, it may be seen as a less pressing case for changing behaviour. Making the desired behaviour change clear, salient and justified can balance out people's tendency to care less about "distant" harms. The availability and prestige of evidence and experience may be crucial factors in doing so.
3. **How the change will be accomplished.** MINDSPACE effects depend at least partly on automatic influences on behaviour. This means that citizens may not fully realise that their behaviour is being changed – or, at least, how it is being changed.

4.2. Influence Strategies

Messages which are most concerned on persuading us, are found in advertising, public relations and advocacy. These "persuaders" use a variety of techniques to grab our attention, to establish credibility and trust, to stimulate desire for the product or policy, and to motivate us to act (buy, vote, give money, etc.).

We call these techniques the "language of persuasion".[1] They're not new. Aristotle wrote about persuasion techniques more than 2000 years ago, and they've been used by speakers, writers, and media makers for even longer than that. The basic persuasion techniques include:

- Fear

[1] Media Literacy Project, Language of Persuasion, Retrieved from http://medialiteracyproject.org/language-persuasion

- Association
- Beautiful people (a way to attract attention)
- Experts
- Explicit claims (So are specific, measurable promises about quality,
- Effectiveness, or reliability)
- Humour
- Intensity (comparatives, exaggeration)
- Testimonial
- Repetition

Intermediate persuasion techniques include:

- Nostalgia
- Rhetorical questions
- Scientific evidence
- Symbols. Symbols are words or images that bring to mind some larger concept, usually one with strong emotional content

Advanced persuasion techniques include:

- Analogy (an analogy compares one situation with another)
- Denial
- Group dynamics
- Majority belief
- Scapegoating
- Timing (Sophisticated ad campaigns commonly roll out carefully-timed phases to grab our attention, stimulate desire, and generate a response).

Clearly, lecturing and other attempts at verbal persuasion haven't managed to effect all of the change we need. Usually, single-source strategies are rarely the answer to complex problems (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

People do not just follow advice or instructions even if they come from a person of authority. Especially, security education is a field that requires background and experience in the varied subject areas within the security environment that are only accomplished through learning over time (Roper et al., 2006).

In many of the cases listed above, end users do know about the dangers. Security experts have warned them, confused them, and filled them with fear, uncertainty and doubt. People base their conscious decisions on whether they have the ability to do what is required and whether the effort will be worth it[2].

[2] Robinson A., The SANS Institute, 2013. https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385

4.3. Factors influencing change

The increased availability of information has significant effects, most of them positive. But providing information per se often has surprisingly modest and sometimes unintended impacts when it attempts to change individuals' behaviour (Dolan, et al., MINDSPACE, 2010).
A considerable amount of money is being spent by Governments on influencing behaviour, and the success in doing so will be maximised if they draw on robust evidence of how people actually behave. Dolan et al., (MINDSPACE, 2010) outline nine robust influences on human behaviour and change.

1. **Messenger** (who communicates information)
2. **Incentives** (our responses to incentives are shaped by predictable mental short cuts, such as strongly avoiding losses)
3. **Norms** (what others do strongly influences us)
4. **Defaults** (we follow pre-set options)
5. **Salience** (what is relevant to us draws our attention)
6. **Priming** (our acts are often influenced by sub-conscious cues)
7. **Affect** (emotional associations can powerfully shape our actions)
8. **Commitments** (we seek to be consistent with our public promises, and reciprocate acts)
9. **Ego** (we act in ways that make us feel better about ourselves)

To really enact change, we must find the current sources of influence-whether they are conscious or unconscious, personal, environmental or social, which are keeping people from enacting vital behaviours (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

Personal motivations refer to feelings associated with an action, while social motivations come from peer pressure and interactions with others in a group. Environmental motivations can be coming either from the physical environment or the ways the culture of an organization rewards and punishes certain activities (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

4.3.1. Personal Factors

The individuals and their knowledge, skills and understanding of cybersecurity as well as their experiences, perceptions, attitudes and beliefs are the main influencers on behaviour (Coventry, et al., 2014, Government Office for Science, UK). Personal motivation and personal ability, are the most powerful sources of influence (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011)**.** Awareness professionals can tap into the source of motivation by linking people's actions to their values. By giving people an image of their best selves, and showing them how to stay true to that image, enacting "secure" behaviours can be made inherently satisfying (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008)**.** When values align with actions, people are more excited to work and be more productive (Meyerson, 2011).

In many cases, people will have to overcome existing patterns in order to form new habits. If asked, the conscious mind will invent stories to rationalize these things that the unconscious mind is telling them to do (Hogan, 2005). The desire to behave consistently will drive people to honour a previous commitment to an ideal or an activity (Cialdini, 2009). As users begin to think of themselves as people who are security-conscious, they then begin to act in accordance with this image.

In many cases, these behavioural changes can lead to attitudinal changes. In order people to change their behaviour they have to start by doing something (Hogan, 2005). If a security practitioner is trying to sell an idea or a behaviour, then first he has to present users with a more difficult, more unpleasant or more expensive behaviour.

Changing the emotion associated with an activity is a powerful way to motivate this change in behaviour (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008). "Vicarious experience", using vivid stories that allow the listener to become a participant by identifying with the characters, is a powerful technique for affecting this emotional change (Hogan, 2005).

4.3.1.1. Security Fatigue[3]

People can sometimes get tired of security procedures and processes, especially if the perception is that security is an obstacle, disturbing them all the time. It can also be stressful to remain at a high level of vigilance and security awareness. These feelings can be a sign of Security Fatigue and they can be hazardous to the overall health of an organization or society.

In the security world there is something called the Security vs. Usability Triangle. The basic premise behind the triangle is that you are trying to create a balance between security and usability. If the triangle leans too far in either direction, then this can lead to a super secure system that no one can use, or an insecure system that everyone can use, even hackers. Therefore, there has to be a balance. Security fatigue becomes an issue when the triangle swings too far to the security side.

If security fatigue sets in at an organizational level, it could cause users and administrators to become lax and could open up the doorways for hackers and malicious social engineers.

4.3.2. Social Factors

Another powerful influence source available to security awareness professionals is peer pressure. The majority of people will conform to the social norm. Leadership is a key component of security culture (Coventry, et al., 2014, Government Office for Science, UK). Influential leaders derive their power from four perceptions (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008):

- They are knowledgeable and continue learning
- They have others' best interests at heart
- They are generous with their time and well connected
- They speak their minds directly

4.3.3. Environmental Factors

To change behaviour, the easiest thing to do may often be to change the environment and make the desired behaviour easier to achieve. Environmental influencers reflect the design of the

[3] O'Donnell Andy, How to Prevent IT 'Security Fatigue. Retrieved from: http://netsecurity.about.com/od/advancedsecurity/a/How-To-Avoid-IT-Security-Fatigue.htm

environment, the physical environment such as the workplace, and the technology, but also the economic factors (Coventry, et al., 2014, Government Office for Science, UK).

4.4. Fear

A meta-analysis (Sutton, 1982) research conducted on communication invoking fear held between 1953 and 1980, showed that increases in perceived level of fear led to increases in the acceptance of the proposed adjustment or behavioural intention.

4.4.1. Fear as a persuasion approach

The invocation of fear is "*a persuasive message designed to scare the world, describing the terrible things that will happen if they do not do what the message recommends*» (Witte, 1992). Surveys have shown that fear can be a quite persuasive tactic to specific situations or counterproductive tactic in other (Ahluwalia, 2000). Psychological research findings show the importance of fear in attitude and / or behaviour change (Levanthal, 1970; Girandola, 2000).

Various theoretical approaches have been used to explain the effect of fear persuasion e.g. The Drive Model-Janis, (1967), The Parallel Reaction Model (Levanthal, 1970) and the Protection Motivation Theory (Rogers, 1975; 1983).

Culturally sensitive interventions have been found to cause more effective changes in behaviour in high-risk populations, such as adolescents. This finding suggests that interventions based on major theoretical knowledge to change behaviour (e.g., social learning theory or the theory of self-efficacy) take into account the cultural beliefs and attitudes, and are more likely to succeed (Arthur, Quester, 2004).

O'Keefe (1990), makes an important distinction between the two definitions of fear invocations (message content - public reactions) and he notes that messages with horrible content may not cause fear and that fear may be caused without frightening contents. However, the majority of research on invoking fear have combined both definitions to handle fear invocations.

When researchers refer to a strong condition of fear invocation, usually they mean that the message represents a big threat and the recipient perceived a big threat. Typically, the invocations of fear offer recommendations that are as efficacious in preventing the threat. Thus, the three central structures in fear invocations is fear, threat and efficacy.

4.5. Control

''Perceived Control'' is a core construct that can be considered as an aspect of empowerment (Eklund, & Backstrom, 2006). It refers to the amount of control that people feel they have, as opposed to the amount of ''Actual Control'' that they have. In contrast, ''Vicarious Control'' and ''Vicarious Perceived Control'' refer to the amount of control that outside entities have over the subject.

The positive effects of perceived control mainly appear in situations where the individual can improve its condition through its own efforts. Also, the greater the actual threat, the greater the

value that perceived control can play. When we apply this theory to information security, we could assume that home computer users often experience high levels of actual control over their risk exposure. They can choose which websites to visit, whether to open email attachments and whether to apply system updates. In contrast, employees in big organisations, lack the sense of control, since IT experts control every aspect of security (More Josh, 2011).

Ajzen (2002), introduced a new concept concerning the relationship between self-efficacy and perceived behavioral control. He argued that "*the central concept of perceived behavioral control consists of two factors: self-efficacy (on the ease / difficulty of performing a behavior) and the ability to control (the extent to which performance depends entirely on the person)*."

5. Culture

Culture is also an important factor that can influence the process of persuasion. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient. As a result, cultural factors are being in consideration when designing messages (Kreuter & McClure, 2004).

The role of culture in the persuasion process is until now under research. How can cultural factors impact the persuasion process? Is persuasiveness of a message determined by the cultural background of the message recipient and its framing in order to be congruent with culturally divergent motivational styles?

Cultural systems shape a variety of psychological processes. Motivational orientation is one potential process behind cultural differences. Messages that match regulatory focus can ''feel right'' and this feeling leads us to an evaluation of the content of the message, which increases persuasiveness (Uskul, A. et. al., 2009).

Messages are more persuasive when there is a match between the recipient's cognitive, affective or motivational characteristics and the content of framing of the message. Also, messages are more persuasive if they match and individual's ought or self-guides, or self-monitoring style (Uskul, A. et. al., 2009).

The Regulatory focus theory (Higgins, 1998), proposes that in a promotion-focused mode of self-regulation, individuals' behaviours are guided by a need for nurturance, the desire to bring one's actual self into alignment with one's ideal self, and the striving to attain gains. In a prevention-focused mode of self-regulation individual's behaviours are guided by a need of security, the need to align one's actual self with one's ought self by fulfilling one's duties and obligations and the striving to ensure non-losses.

The values that distinguish country cultures from each other could be categorised into four groups (Hofstede at al., 2010)[4]. The Hofstede dimensions of national culture are a) Power Distance (PDI) b) Individualism versus Collectivism (IDV) c) Masculinity versus Femininity (MAS) and d)Uncertainty Avoidance (UAI). Culture can be only used meaningfully by comparison. The forces that cause cultures to shift tend to be global or continent-wide. This means that they affect many countries at the same time, so if their cultures shift, they shift together and their relative positions remain the same. Exceptions to this rule are failed states and societies in which the levels of wealth and education increase very rapidly.

In Western more individualistic cultures, people tend to define themselves in terms of their internal attributes such as goals, preferences and attitudes. Individuals tend to focus on their personal achievements and tend to favour promotion over prevention strategies focusing on positive outcomes that they hope to approach, rather than the negative outcomes they hope to avoid (Lockwood, Marshall, & Sadler, 2005). Providing messages that fit the dominant regulatory focus of individuals may lead to a ''feeling right'' experience and thus to an increased persuasion (Cesario et al., 2004).

[4] http://geert-hofstede.com/national-culture.html

In Eastern more collectivist cultures, individuals tend to define themselves in terms of their relationships and social group memberships (Triandis, 1989). In this cultural context, individuals tend to avoid behaviours that cause social disruptions and they favour prevention over promotion strategies focusing on the negative outcomes which they hope to avoid rather than the positive outcomes they hope to approach (Lockwood et al., 2005).

5.1. Culture and Risk perception

Risk perception refers to people's responses to questions regarding the riskiness of their decisions and actions (Weber E. & Hsee Ch., 2000). Perception of risk can be a collective phenomenon (Douglas, M., & Wildavsky, A., 1982). Each culture selects some risks for attention and chooses to ignore others.

Cultural differences in risk perceptions are explained in terms of their contribution to maintaining a particular way of life. There are different patterns of interpersonal relationships such as archical, individualist, egalitarian, fatalist and hermitic. Risk is also seen as the other side of trust and confidence, as the result of the way in which the theory see risk perception as being imbedded in social relations (Douglas, M., & Wildavsky, A., 1982).

6. Rewards and Punishments

Rewards and punishments can be used in order to influence people follow a desired behaviour. Both rewards and punishments, however, can have unintended consequences[5]. Rewarding people for an activity that they already enjoy makes that activity less desirable, while the receiver of the reward begins to question the intrinsic value of the activity (Kohn, 1994). Even honouring certain employees that follow the new standards may backfire, causing others to feel resentful (Patterson, Gremm, Maxfield, McMillan & Switzler, 2008).

This process is called, "Incentivized Awareness Programs" (Winkler & Manke, 2013)[6]. That better represents what we are talking about, as a comprehensive awareness program does not limit itself to a single tool. With incentivized awareness (Gamification), you create a reward structure that incentivizes people to exercise the desired behaviours, which could include seeking out additional training. The incentives ideally make demonstrating or learning about awareness behaviours fun.

Rewarding people for doing the right behaviours makes them more security conscious. In general, extrinsic rewards should not be the first strategy. They could be used them only in conjunction with motivational strategies that encourage intrinsic satisfaction and social support (Kohn, 1994). Short-term goals need to be created and small improvements in those vital behaviours can be celebrated.

Economists argue that we are more inclined to avoid actual loss than to strive for conditional benefits. This tendency is called loss aversion and it refers to not setting the stakes too high.

[5] Robinson A., Using influence strategies to improve security awareness programs, The SANS Institute, 2013. Retrieved from: https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385

[6] Winkler & Manke (2013).

1. 7. Media-Framed Messages

Media constructions often serve as a heuristic for citizens, whose understanding of issues is powerfully shaped by the values involved (Domke D. et al., 1998). Prevention messages typically try to convey either the benefits of performing a behaviour (gain-framed messages) or the costs associated with failing to perform a health-promoting behaviour. Gain-framed messages are usually more persuasive when they are used to promote prevention behaviours. Messages which are congruent with a person's predominant motivational orientation are more effective than messages that are not congruent.

Most studies on framing have compared the persuasive power of messages emphasizing the benefits of performing a behaviour, to messages highlighting the cost of not performing a behaviour (similar framing effects). The distinction between positive and negative messages, with respect to either the presence or absence of pleasant or unpleasant results seem to be a useful conceptual tool for studying the role of pre-existing perceptions about safety issues. Broemer, P. (2002), states that the framework would be relevant even when given only negative results.

2. 8. Essential Components for a Campaign

In order a Campaign to be successful, there are several essential components which need to be taken into consideration (Winkler Ira and Manke Samantha, 2013)[7].

1. **Communication**. A significant part of a campaign is communication. This can be accomplished by collateral, internally distributed materials. These are things like newsletters, blogs, and other internal communications. Also, posters are a very crucial method of raising awareness. While some people believe they are old-fashioned and outdated, they can be very effective when they are well designed.
2. **Computer Based Training.** CBT is the most omnipresent component of security awareness programs, as it is the most clearly accepted method of achieving compliance.
3. **Events.** Well-executed events bring the Security Awareness program, and the whole security effort for that matter, to life.
4. **Security Portal.** An internal security portal provides several functions. It provides a Knowledge base that can provide a huge return on investment with includes information on security related topics. It is also important to include information on home and personal security strategies, such as protecting children online and securing social media accounts.
5. **Behavioural Testing and Teachable Moments.** Phishing, USB drive drops, and Social Engineering tests require some care, but are important components to give your employees a "teachable moment."
6. **Teaching New Skills Effectively**. What looks like a lack of motivation is sometimes really a lack of ability (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011). As teachers, security awareness professionals must break down complex goals in short, clear achievable steps.

[7] Winkler & Manke (2013).

3. 9. Factors which lead to a Campaign's failure

In order a Campaign to be successful, there are several factors which need to be avoided (Winkler and Manke, 2013)[8].

1. **Not understanding what security awareness really is.** Information must be provided in a way that relates to how people think and behave. There must be a personal association of how knowledge would impact their actions. There is also a difference in providing an individual information on a one time basis, and delivering information in different formats over the course of time to effect change.
2. **Compliance.** In short, saying your awareness program is compliant does not necessarily equate to create the desired behaviours.
3. **Illustrate that awareness is a unique discipline.** A good security awareness professional will have good communication ability, be familiar with learning concepts, understand that awareness is more than a check the box activity, knowledge of a variety of techniques and awareness tools, and an understanding that there is a need for constant reinforcement of the desired behaviours.
4. **Lack of engaging and appropriate materials.**
5. **Not collecting metrics.** By collecting regular metrics, you can adjust your program to the measured effectiveness. By determining what is working and what is not, you can tailor future programs based upon lessons learned. The appropriate metrics also allow for the determination of which components are having the desired impact. They should be taken prior to starting any engagement effort, at least once during the engagement, and also post-engagement.
6. **Unreasonable expectations**. No security countermeasure will ever be completely successful at mitigating all incidents. There will always be a failure.
7. **Arrange multiple training exercises**. Focusing on a specific topic or threat does not offer the overall training needed.

[8] Winkler & Manke (2013).

4. 10. Case Studies

10.1. Cyber Security Awareness Campaigns in U.K.

10.1.1. GetSafeOnline Campaign[9]

This campaign focuses on users at home and businesses. Get Safe Online is a jointly funded initiative between several Government departments and private sector businesses. It provides practical advice on how to protect yourself, your computers and mobiles device and your business against fraud, identity theft, viruses and many other problems encountered online. It contains guidance on many other related subjects too – including performing backups and how to avoid theft or loss of your computer, smartphone or tablet. Every conceivable topic is included on the site – including safe online shopping, gaming and dating. The site also keeps you up to date with news, tips and stories from around the world. Unfortunately, there is too little information regarding cyberbullying and how to act when you are a victim.
The site offers easy access by listing information. All information appears on the home page. Also a question Fag and possibility to apply your own question.

Message: The positive message of ''get safe online'' again gives the responsibility to users for staying safe.
The campaign covers, topics such as:

- Protecting Your Computer
- Protecting Yourself
- Smartphones & Tablets
- Shopping, Banking & Payments
- Safeguarding Children
- Social Networking
- Businesses

The campaign offers a repository of threats and how-to advice but its tone and approach is based on essential fear tactics. As previously discussed, messages with horrible content may not cause fear and that fear may be caused without frightening contents. Fear invocations cannot be successful in changing behaviour if the three central structures of fear invocations - fear, threat and efficacy - are combined.

It is very important to embed positive information security behaviours, which can result to thinking becoming a habit. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient. Messages also can be more persuasive when there is a match between the recipient's cognitive, affective or motivational characteristics and the content of framing of the message.

[9] www.getsafeonline.org

10.1.2. The 'Cyber Streetwise' campaign[10]

This campaign focuses on users at home and businesses. The campaign advices home users to use social media responsibly, to keep a child's identity safe. In short, this campaign presents users as the weakest links in the cyber security chain.

The new Home Office Cyber Streetwise site advises businesses to adopt five basic measures. These include, using strong, memorable passwords, installing antivirus software on all work devices, checking privacy settings on social media, checking the security of online retailers before loading card details and patching systems as soon as updates are available. The service will be of particular use to small and medium-sized businesses.

A survey of FTSE 350 companies by the Department for Business, Innovation and Skills last month revealed that only 14 per cent are regularly considering cyber threats, with a significant number not receiving any intelligence about cyber criminals.

It is a campaign which tries to cause a behavioural change by providing tips and advice on how to improve online security.

- It urges businesses to get online
- To take control of their online behaviour
- Suggests to companies that a well-designed site provides a sense of security and business reliability.
- Suggests that the good reputation of a company for safety and security online will lead to business growth and will boost sales.

Message: The campaign uses a positive message method to influence the behaviour of users. ''*In short, the weakest links in the cyber security chain are you and me*''. This campaign represents several advances on past government-supported efforts:

1. The campaign targets specific demographic groups: based on Experian's MOSAIC product of UK demographics, X target users groups have been identified by age, gender and education/profession: small and medium businesses, seniors, middle aged men who know it all, etc.). Specific cyber threats, and how to protect against them been designed by communication professionals, is visually appealing and engaging, and avoids the 'scare factor'. It also presents the materials in the context of everyday tasks that people recognise: banking
2. The effect of targeted campaigns is measured through a set of Key Performance Indicators (KPI) for secure online behaviours.

The campaign covers, topics such as:

1. Passwords
2. Bank safely online / on your mobile
3. Common shopping scams
4. Computer health
5. Identity theft

[10] www.cyberstreetwise.com

6. Operating system and software updates
7. Online payment options
8. Online shopping
9. Phishing
10. Social media
11. Smart phone health
12. Wireless network security

These are the main advice suggestions on security for users. The advice usually comes from security experts and service providers, who monotonically repeat suggestions such as 'use strong passwords'. That advice pushes responsibility and workload for issues that should be done by the service providers and product vendors onto users, not caring that following this advice would be a near-full-time job for those who can understand it.

One of the main reasons why users do not behave optimally is that security systems and policies are poorly designed. Security awareness, education and training cannot just 'fix' security problems (Coventry, et al., 2014, Government Office for Science, UK). If security is difficult to use, too complex, too effortful, people will not do it. Perceived control, the sense one has that he/she can drive specific behaviour has been found to affect the intention of behaviour but also the real behaviour. Currently users' time and goodwill is being wasted on security that is too difficult to use, and not effective (Kirlappos, I., & Sasse, M. A., 2012).

10.1.3. Webwise Campaign[11]

This campaign focuses mainly on parents and home users. It provides basic knowledge on various cyber risks and basic protection tips. The site offers Information, games, news, resources and video relating to disability.

Message: The campaign urges users to *''Make the most of being online''*. It offers an online course, whereas basic technology is used.

The campaign covers, topics such as:

- Home
- Your computer
- Using the web
- Email & sharing
- Living & interests
- Safety & privacy
- Glossary

[11] http://www.bbc.co.uk/webwise/0/

1.1.4. Good to know Google's[12]

This campaign targets the general public but mainly families. It provides basic knowledge on various cyber risks and basic protection tips. The site offers Information, games, news, resources and video relating to disability.

Message: The campaign uses a more collective/collaborative message ''*Working together to stay safe online*''. It is friendly to users with a step by step guide.

The campaign covers, topics such as:

- Manage your privacy and security
- Prevent cybercrime
- Getting started
- Explore with confidence
- Manage your online reputation

Google launched the "*Good to Know*" campaign promoting online safety in association with the Citizens Advice Bureau (CAB).

10.1.5. Behind the Screen[13]

Behind the Screen is a hub of free computing resources for your GCSE students, complete with lesson plans and mark schemes. The resources are developed with industry to provide authentic projects mapped to computing, ICT and computer science qualifications.

The Behind the Screen projects and resources are currently free to use for all UK schools. There are eight projects live on the site. Projects are developed with key industry partners who provide the real life business cases and ideas for each, and supply industry resources and software for students to use. Projects are presented as problems through a brief, and students are guided through to their solution. All resources they need to achieve the outcomes are provided. Projects take from 6 to 15 hours to complete, depending on the route taken. Extension activities are also provided.

Projects are supported with lesson plans, guides, mapping to current Key Stage 4 qualifications, and presentations to support delivery. Assessment is through a Student Log, and teachers are provided with an exemplar to make assessment straightforward.

10.1.6. Cyber Security Challenge UK[14]

Cyber Security Challenge UK is helping to fill the cyber security skills gap by tapping into untapped talent. It is a not-for-profit organisation which operates primarily through sponsorship. Its main role is to run a national programme of competitions which are designed to attract and inspire new talent into the UK cyber security profession.

---

[12] https://www.google.co.uk/goodtoknow/
[13] http://www.behindthescreen.org.uk/
[14] http://www.cesg.gov.uk/awarenesstraining/Pages/Cyber-Security-Challenge-UK.aspx

Sponsored by over 50 organisations from government, industry and academia and leading sponsor Government Communications Headquarters (GCHQ), the Challenge sets competitions that test existing cyber security skills, runs cyber camps to help individuals develop new skills, and provides information through networking events on cyber security career changes.

CESG have produced two posters for the Palace of Westminster to help raise IA awareness which can be customised with your own logo for use in your own government department (or supporting industry partner).

10.1.7. The Devil's In Your Details[15]

In the first campaign of its kind involving both the private and public sectors, The Devil's in Your Details campaign brings together Action Fraud, The Telecommunications UK Fraud Forum (TUFF) and Financial Fraud Action UK - the name under which the financial services industry coordinates its fraud prevention activity, in a powerful demonstration of what can be achieved when industry and government work together.

The National Fraud Authority backed campaign is raising awareness of the importance of protecting personal information and aims to remind the public to check that who they share their details with is genuine**.** The Devil's In Your Details campaign encourages consumers to suspect anyone or anything they are uncertain about, to keep asking questions and to challenge or end an engagement if it feels uncomfortable. As an introduction to a wider campaign against fraud, this awareness activity aims to increase reporting of fraud, making it harder for fraudsters to target consumers in the future.

The campaign includes professional videos which are very well presented. But it scared less experienced people away from online transactions, which is not what government intends to achieve. Fear invocations cannot be successful in changing behaviour if the three central structures of fear invocations - fear, threat and efficacy - are combined. It is crucial to decide the target group of a campaign and try to match a cultural theme of the message recipient but also match the recipient's cognitive, affective or motivational characteristics with the content of framing of the message.

It is very important to embed positive information security behaviours, which can result to thinking becoming a habit, instead of using fear invocations often leading to pure avoidance of the suggestion.

10.1.8. VOME[16] Visualisation and Other Methods of Expression

VOME is a three year collaborative research project bringing together researchers from the Information Security Group (ISG) at Royal Holloway, University of London, Salford and Cranfield Universities, working with consent and privacy specialists at Consult Hyperion and Sunderland City Council, to explore how people engage with concepts of information privacy and consent in on-line interactions.

[15] http://www.actionfraud.police.uk/thedevilsinyourdetails
[16] http://www.vome.org.uk/

The purpose of VOME (Visualisation and Other Methods of Expression) is to explore how user communities engage with concepts of information privacy and consent in on-line interactions. The aim is to develop alternative conceptual models of on-line privacy which enable users to make clearer on-line disclosure choices. These decision making models will facilitate a better dialogue between the designers of privacy and consent functionality and their customers.

This project offers benefits to on-line service providers, the manufacturers of technology used to deploy on-line services, as well as the general public. To date there has been considerable interest in this project from each of these communities.

This is a more innovative approach to raising awareness including games, theatre and other methods of expression.

10.2. Cyber Security Awareness Campaigns in Australia

10.2.1. Stay Smart Online[17]

This is a one-stop shop providing information for Australian Internet users on the simple steps they can take to protect their personal and financial information online. The site has informative videos, quizzes and a free Alert Service that provides information on the latest threats and vulnerabilities**.**

10.2.2. ThinkUKnow - Internet Safety Program[18]

ThinkUKnow is an Internet safety program delivering interactive training to parents, carers and teachers. Created by the UK Child Exploitation and Online Protection (CEOP) Centre, ThinkUKnow Australia has been developed by the Australian Federal Police (AFP) and Microsoft Australia. Users will need to subscribe to the site to gain access to its tools and resources.

10.2.3. Tagged (CyberSmart) - ACMA[19]

Developed by the ACMA's Cybersmart program, Tagged has received acclaim for its realistic depiction of teenagers and the problems they can face in a digital world. Since its launch in September 2011, Tagged has become a popular resource for Australian teachers and parents. More than 10,000 copies of the film and posters have been distributed nationwide and it has attracted nearly 50,000 views on YouTube.

10.2.4. Smart online, safe offline (SOSO) - National Association for Prevention of Child Abuse and Neglect (NAPCAN)[20]

By using social networking environments to target children and young people directly, the SOSO initiative educates children and young people about the dangers that exist online and on how they can manage their personal safety.

[17] http://www.staysmartonline.gov.au/
[18] http://www.thinkuknow.org.au/site/
[19] http://www.cybersmart.gov.au/Home/Teens/Games%20and%20videos/tagged.aspx
[20] http://napcan.profero.com.au/soso

10.2.5. Make cyberspace a better place - KIDS Helpline[21]

Kids Helpline campaigns to help children enjoy the freedom and fun of using the Internet and to and help make cyberspace a fun and safe place.

10.2.6. The Alannah & Madeline Foundation - Keeping children safe from violence[22]

This national charity aims to protect children from violence and its devastating impact. The website provides a range of information and resources for parents and children, including an evidence-based educational program (eSmart Schools), and a variety of other resources about bullying and cybersafety.

Some campaigns are delivered in collaboration with a wide variety of public and private agencies. As a result, there is a large degree of crossover in the material of various contributors presented across the websites. Furthermore, initiatives may target a specific issue (such as cyberbullying), or they may be delivered as part of a broader social awareness campaign (child protection).

10.2.7. Who's chatting to your kids? - Queensland Police Resource[23]

A brochure published by the Queensland Police Service's Task Force Argos. This brochure provides information to parents on Internet safety for children and young people. It discusses social networking, mobile phones, webcams and online gaming, and provides information about the types of things to look out for that may indicate that children could be at risk.

Some of the more popular social networking sites provide information specifically tailored to help parents understand their child's use of the site.

10.2.8. Keep it Tame[24]

Keep it Tame Campaign tries to Promote Online Safety and Measure Behaviour Change in Young People. This is an online campaign targeting Australian teenagers, drawing attention to the consequences of thoughtless and hurtful use of social media and empowering them to act with respect online.

Unique to the campaign is the application of an innovative digital tracking methodology which – in conjunction with a cohort study that will survey and interview young people over time – will measure its impact on behaviour change.

The campaign guides teenagers through a series of mock social media posts. As things turn nasty, an animated creature slowly becomes more grotesque, highlighting the hurtful effects of the online exchanges and ultimately encouraging people to act with respect. The Keep it Tame

[21] http://www.kidshelp.com.au/teens/get-info/cyberspace/
[22] http://www.amf.org.au/bullying/
[23] http://www.police.qld.gov.au/programs/cscp/personalSafety/children/childProtection/
[24] http://www.youngandwellcrc.org.au/keep-tame-campaign-promote-online-safety-measure-behaviour- change-young-people/

campaign is the first in a series of campaigns to come out of the Young and Well CRC'sSafe and Well Online project, a five-year study of the most effective ways to design, deliver and evaluate online social marketing campaigns aimed at improving safety and wellbeing.

This project is an initiative of the Young and Well CRC and is led by the University of South Australia in conjunction with the University of Western Sydney, Zuni and the Queensland University of Technology. Safe and Well Online builds upon the original Smart Online Safe Offline initiative developed by NAPCAN.

10.3. Cyber Security Awareness Campaigns in Canada

10.3.1. Get Cyber Safe[25]

Get Cyber Safe is a national public awareness campaign created to educate Canadians about Internet security and the simple steps they can take to protect themselves online. The campaign's goal is to bring together all levels of government, the public and private sectors, and the international community, to help Canadians be safer online.

The campaign is an important component of Canada's Cyber Security Strategy, which is dedicated to securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online.

The campaign is being led by Public Safety Canada on behalf of the Government of Canada.

10.3.2. Stop Hating Online[26]

Stop Hating Online is the Government of Canada's anti-cyberbullying public awareness campaign. It focuses on cyberbullying in terms of social impacts and potential legal consequences. As a comprehensive resource for parents and youth, GetCyberSafe.ca provides information, advice and tools to prevent and stop hate, cyberbullying and the non-consensual distribution of intimate images that can take place online, including through social networks and mobile messages. The campaign encourages everyone to stand up against cyberbullying.

10.4. Cyber Security Awareness Campaigns in Africa

10.4.1. ISC Africa[27]

A coordinated, industry and community-wide effort to inform and educate Africa's citizens on safe and responsible use of computers and the internet so that we can minimise the inherent risks and increase consumer trust.

[25] http://www.getcybersafe.gc.ca/cnt/bt/index-eng.aspx
[26] http://www.getcybersafe.gc.ca/cnt/blg/pst-20140109-eng.aspx
[27] http://iscafrica.net/#home

10.4.2. Parents corner[28]

The effort is intended to co-ordinate the work done by government, industry and civil society. Its objectives are to protect children, empower parents, educate children and create partnerships and collaboration amongst concerned stakeholders. Parents' Corner tips for a safer internet include:

1. People aren't always who they say they are.
2. Think before you post.
3. Likewise, children need to think before they respond to things that other people have posted.
4. It's not just about computers. Many parents don't understand that the Internet their children can access via their cell phones is the same Internet accessed via a computer.
5. Finally, just as they would in real life, friends must protect friends.

[28] http://www.parentscorner.org.za/

11. Conclusions

The ISF report (February 2014), proposes that simple transfer of knowledge is not enough. Knowledge and awareness is a prerequisite to change behaviour but not necessarily sufficient and this is why it has to be implemented in conjunction with other influencing strategies. It is very important to embed positive information security behaviours, which can result to thinking becoming a habit, and a part of an organisation's information security culture. One of the main reasons why users do not behave optimally is that security systems and policies are poorly designed.

Moreover, the advice usually comes from security experts and service providers, who monotonically repeat suggestions such as 'use strong passwords'. But, security awareness, education and training cannot just 'fix' security problems. If security is difficult to use, too complex, too effortful, people will just not accept it (Coventry, et al., 2014, Government Office for Science, UK). Currently users' time and goodwill is being wasted on security that is too difficult to use, and not effective (Kirlappos, I., & Sasse, M. A., 2012). Behaviour change in an information security context could be measured through risk reduction, but not through what people know, what they ignore or what they do not know.

Culture is also an important factor that can influence the process of persuasion. Messages and advertisements are usually preferred when they match a cultural theme of the message recipient. As a result, cultural factors are being in consideration when designing messages (Kreuter & McClure, 2004). Messages also can be more persuasive when there is a match between the recipient's cognitive, affective or motivational characteristics and the content of framing of the message. Also, messages are more persuasive if they match and individual's ought or self-guides, or self-monitoring style (Uskul, A. et. al., 2009).

As previously discussed while reviewing existing awareness campaigns fear invocations are often used, as influence strategies. But, fear invocations are proved insufficient to change behaviour. They cannot be successful in changing behaviour if the three central structures of fear invocations - fear, threat and efficacy - are not combined. As previously discussed, messages with horrible content may not cause fear and fear may be caused without frightening contents.

Following that rationale of the expected utility approach, perhaps increasing the 'perceived utility' of cybersecurity could be one additional factor to improve the effectivity of awareness campaigns. Also, perceived control and personal handling ability, the sense one has that he/she can drive specific behaviour has been found to affect the intention of behaviour but also the real behaviour. A campaign should use simple consistent rules of behaviour that people can follow. This way, their perception of control will lead to better acceptance of the suggested behaviour.

We suggest that the following factors can lead to more sufficient awareness campaigns:

1. Awareness has to be professionally prepared and organised in order to work.
2. Causing feelings of fear to people is not an effective tactic, since it will put off people who can least afford to take risks. To make the internet accessible, risks should not be exaggerated.
3. Awareness alone is not enough. Usually all it does is catch attention.

4. Security education has to be more than providing information to people - it needs to be targeted, actionable, and doable. At the moment, what is correct behaviour is far too difficult and complex. We need simple consistent rules of behaviour that people can follow.
5. Once people are willing to change, training and feedback is needed to sustain them through the change period.

References

Ajzen, I. (1988). Attitudes, personality, and behaviour. Dorsey Press, Chicago.

Bernoulli, Daniel, "Exposition of a New Theory on the Measurement of Risk". Originally published in 1738, translated by Dr. Louise Sommer. (January 1954). *Econometrica* (The Econometric Society) **22** (1): 22–36. doi:10.2307/1909829.

Caputo, D., Lawrence Pfleeger, Sh., Freeman, D.J., Johnson, E.M. Going Spear Phishing: Exploring Embedded Training and Awareness, IEEE Security & Privacy, vol. 12, no. 1, pp. 28-38, Jan.-Feb. 2014, doi:10.1109/MSP.2013.106.

Cesario, J., Grant, H., & Higgins, T.E. (2004). Regulatory fit and persuasion: Transfer from ''feeling right''. *Journal of Personality and Social Psychology, 86,* 388-404.

Cook, T., & Flay, B. (1978). The temporal persistence of experimentally induced attitude change: An evaluative review. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (vol. 11). New York: Academic Press.

Coventry, D.L., Briggs, P., Blythe, J., Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. Government Office for Science, London, UK. Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf

Dolan P., Hallsworth, M., Halpern, D., King,D., Vlaev, I. MINDSPACE Influencing behaviour through public policy, Institute for Government, Cabinet Office, 2 March 2010. Retrieved from: http://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf

Domke David, Shah V. Dhavan and Wackman B. Daniel (1998). Media Priming Effects: Accessibility, Association and Activation. *International Journal of Public Opinion Research, 1(1),* 51-74.

Douglas, M., & Wildavsky, A. (1982). *Risk and culture: An essay on the selection of technological and environmental dangers.* Berkeley: University of California Press.

Eklund, M., & Backstrom, M. (2006). The role of perceived control for the perception of health by patients with persistent mental illness. *Scandinavian Journal of Occupational Therapy, 13,* 249-256.
Fogg, B. J. (2002). Persuasive Technology: Using Computers to Change What We Think and Do. Morgan Kaufmann.

Fisher, E.B., & Rost, K. (1986).Smoking cessation: A practical guide for the physician. *Clinics in Chest Medicine, 7,* 551-565. Hofstede, G., Hofstede, J.G., Minkov, M. Cultures and Organizations: Software of the Mind. 3rd Edition, McGraw-Hill USA, 2010.

Higgins, E.T. (1998). Promotion and prevention: Regulatory focus as a motivational principle. *Advances in Experimental Social Psychology, 30*, 1-46.

Information Security Forum (ISF). From Promoting Awareness to Embedding Behaviours, Secure by choice not by chance, February 2014. Retrieved from: https://www.securityforum.org/shop/p-71-170

Kirlappos, I., Sasse, M. A. (2012). Security Education against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security and Privacy Magazine* 10(2), 24-32

Kirlappos, I., Parkin, S., Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. *Workshop on Usable Security*Kreuter, M. W., & McClure, S. M. (2004). The role of culture in health communication. *Annual Review of Public Health, 25*, 439-455.

Lapowsky Issie (2013). Reward vs. Punishment: What Motivates People More? Retrieved from: http://www.inc.com/magazine/201304/issie-lapowsky/get-more-done-dont-reward-failure.html

Lockwood, P., Marshall, T., & Sadler, P. (2005). Promoting success or preventing failure: Cultural differences in motivation by positive and negative role models. *Personality and Social Psychology Bulletin, 31,* 379-392.

Media Literacy Project, Language of Persuasion, Retrieved from http://medialiteracyproject.org/language-persuasion

More Josh (2011). Measuring Psychological Variables of Control In Information Security, - January 12, Retrieved from http://www.sans.org/reading-room/whitepapers/awareness/measuring-psychological-variables-control-information-security-33594

NIST, National Institute of Standards and Technology. Building an Information Technology Security Awareness and Training Program. Wilson, M. and Hash, J. Computer Security Division Information Technology Laboratory. October 2003. Retrieved from:http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

O'Donnell Andy, How to Prevent IT 'Security Fatigue. Retrieved from: http://netsecurity.about.com/od/advancedsecurity/a/How-To-Avoid-IT-Security-Fatigue.htm

Palmer, C.G.S. (1996). Risk perception: An empirical study of the relationship between worldview and the risk construct. *Risk Analysis, 16*, 717-724.

Robinson Alyssa, Using influence strategies to improve security awareness programs, The SANS Institute, 2013. Retrieved from: https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385

Roper, C., Fischer, L., Grau, J. Security Awareness, Education and Training, Elsevier Inc. UK, 2006. ISBN-13: 978-0750678032.

Simons-Morton, B.G., Donohew, L.C., Aria, D. (1997). Health communication in the prevention of alcohol, tobacco and drug use. *Health Education and Behaviour, 24,* 544-554.

Triandis, H.C. (1989). The self and social behaviour in differing cultural contexts. *Psychological Review, 96,* 506-520.

Uskul K. Ayse, Sherman K. David, Fitzgibbon John (2009).The cultural congruency effect: Culture, regulatory focus, and the effectiveness of gain- vs. loss- framed health messages. *Journal of Experimental Social Psychology, 45,* 535-541. doi: 10.1016/j.jesp.2008.12.005

Weber U. Elke, Hsee K. Christopher (2000). Culture and Individual Judgement and Decision Making. *Applied Psychology: An International Review, 49(1),* 32-61.

Winkler Ira and Manke Samantha (2013). 7 Reasons for Security Awareness Failure, CSO Magazine, July 10. Retrieved from http://www.csoonline.com/article/2133408/network-security/the-7-elements-of-a-successful-security-awareness-program.html

Winkler Ira and Manke Samantha (2013). 6 essential components for security awareness programs. Retrieved from http://www.csoonline.com/article/2133971/strategic-planning-erm/6-essential-components-for-security-awareness-programs.html

Winkler Ira and Manke Samantha (2013). How to create security awareness with incentives. Retrieved from http://www.csoonline.com/article/2134189/strategic-planning-erm/how-to-create-security-awareness-with-incentives.html

Links to Campaigns in U.K.

1. **The 'Cyber Streetwise' campaign** www.cyberstreetwise.com

2. **GetSafeOnline Campaign** www.getsafeonline.org

3. **Webwise Campaign** http://www.bbc.co.uk/webwise/0/

4. **Good to know Google's** https://www.google.co.uk/goodtoknow/

5. **Behind the Screen** http://www.behindthescreen.org.uk/

6. **Cyber Security Challenge UK**
7. http://www.cesg.gov.uk/awarenesstraining/Pages/Cyber-Security-Challenge-UK.aspx

8. **The Devil's In Your Details** http://www.actionfraud.police.uk/thedevilsinyourdetails

9. **VOME Visualisation and Other Methods of Expression** http://www.vome.org.uk/

Links to Campaigns in Australia

1. **Stay Smart Online** http://www.staysmartonline.gov.au/

2. **ThinkUKnow - Internet Safety Program** http://www.thinkuknow.org.au/site/

3. **Tagged (CyberSmart) – ACMA** http://www.cybersmart.gov.au/Home/Teens/Games%20and%20videos/tagged.aspx

4. **Smart online, safe offline (SOSO) - National Association for Prevention of Child Abuse and Neglect (NAPCAN)** http://napcan.profero.com.au/soso

5. **Make cyberspace a better place - KIDS Helpline** http://www.kidshelp.com.au/teens/get-info/cyberspace/

6. **The Alannah & Madeline Foundation - Keeping children safe from violence** http://www.amf.org.au/bullying/

7. **Who's chatting to your kids? - Queensland Police Resource**
8. http://www.police.qld.gov.au/programs/cscp/personalSafety/children/childProtection/

9. **Keep it Tame** http://www.youngandwellcrc.org.au/keep-tame-campaign-promote-online-safety-measure-behaviour- change-young-people/

Links to Campaigns in Canada

1. **Get Cyber Safe** http://www.getcybersafe.gc.ca/cnt/bt/index-eng.aspx

2. **Stop Hating Online** http://www.getcybersafe.gc.ca/cnt/blg/pst-20140109-eng.aspx

Links to Campaigns in Africa

1. **ISC Africa** http://iscafrica.net/#home

2. **Parents corner** http://www.parentscorner.org.za/

IECC Public Awareness and Training Working Group

Cybersecurity Public Relations Plan

June 2018

Indiana Executive Council on Cybersecurity

Public Awareness and Training Plan

2018-2020

Public Awareness and Training Working Group

June 2018

TABLE OF CONTENTS

TITLE	PAGE
EXECUTIVE SUMMARY …….	3
INTRODUCTION ……	4
PURPOSE AND BACKGROUND ……	5
RESEARCH …….	6
CAMPAIGN GOALS …….	13
KEY PUBLICS ……	14
PLAN: PHASE 1 ……..	15
PLAN: PHASE 2 ……..	36
PLAN: PHASE 3 ……..	45
BUDGET …….	54

EXECUTIVE SUMMARY

This cybersecurity plan is developed by the Public Awareness and Training Working Group in support of the Indiana Executive Council on Cybersecurity's (Council) mission. It is designed to increase public awareness, knowledge and positive cybersecurity behaviors by Hoosiers over a five-year period. Additionally, it promotes cybersecurity as a career field for young people and has elements informing the Indiana public about the activities of the Council.

Extensive secondary research demonstrates that similar campaigns to impact public awareness fail. Research has identified that there are 13 key knowledge points (Pew) the public should know and use, and that positively framed messaging is more effective than negatively framed (fear) messaging for influencing behaviors.

Based on the research, a five-year, three-phased plan has been developed to affect behavior change in Hoosier's use of the internet and in their awareness and knowledge of cybersecurity.

A series of overarching goals are established to achieve these changes. Five key publics (audiences) were identified to be reached via a variety of messaging strategies. In each case (publics), measurable objectives are established. Based on the 13 key knowledge points, the public (as organized into the five categories) will be targeted with strategic communication messages to increase awareness and knowledge of cybersecurity practices, and to increase positive behaviors in cybersecurity protection and defense.

Activities will be measured at the conclusion of each phase of the campaign, and the subsequent phase adjusted to reflect that learning.

Two additional goals are established: one to increase knowledge and awareness among high school students about the potential for cybersecurity as a career field, and a second to inform the Indiana public about the activities of the Cybersecurity Council.

The Working Group continues to research and address the career field and training challenges and expects to provide additional materials to support this effort.

This plan is the result of approximately a year of effort on behalf of the Working Group to develop. The Group will continue to work on projects in support of the overall Cybersecurity Council mission, including development of training options, and providing advice and counsel to other committees and working groups as needed. It will also serve as an advisory group during the implementation of this campaign plan as needed.

Indiana Executive Council on Cybersecurity
Public Awareness and Training Plan
2018-2020

July 2018

INTRODUCTION

This cybersecurity plan is presented in partial fulfillment of the Public Awareness and Training Working Group's mission. It includes a detailed research summary, a detailed set of goals and objectives, and a three-phased campaign plan to increase awareness, knowledge and positive cybersecurity behaviors among five key publics in Indiana.

This plan is the result of approximately a year of effort on behalf of the Working Group to develop. The Working Group anticipated that execution of this campaign plan would be the responsibility of state government agencies, either directly or with a third-party agency (advertising/public relations contractor), and under the direction of a state official.

The Group will continue to work on projects in support of the overall Council mission, including development of training options, and providing advice and counsel to other committees and working groups as needed. It will also serve as an advisory group during the implementation of this campaign plan as needed.

It should be noted that the plan addresses Indiana residents in four categories. In one category, the intent is to inform Indiana residents about the activities of the Council. That function is addressed in the plan, but not fully developed. It is anticipated a separate plan will be developed via the Governor's office, IOT, Homeland Security and others to address that goal in greater detail.

Additionally, we did not address the need to properly "brand" the Council's efforts. However, the Working Group strongly recommends that take place to support the effort and to separate the state's work and messages from others. Branding also identifies the state's efforts to do so via this campaign.

PURPOSE

The Public Awareness and Training Working Group of the Indiana Executive Council on Cybersecurity (Council) has been charged by Governor Holcomb to create an executable plan to communicate cybersecurity awareness and knowledge to citizens of Indiana. The Council was established by Executive Order #17-11 dated January 9, 2017.

> The Council's mission:
> The Council shall develop, maintain, and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe.
>
> Working Group Mission:
> In order to protect the security and economy of the State, it is appropriate and necessary for state government to establish and lead a statewide, collaborative effort involving government, private-sector, military, research, and academic stakeholders to enhance Indiana's cybersecurity.

The working Group established three principle goals for its work. The goal specifically addressed by this plan is:

> Develop a comprehensive plan to provide information and training to the public in general and specific sectors of the Indiana economy to protect its electronic data from criminal or terroristic attempts to breach electronic databases and what to do if a breach does occur.

BACKGROUND

The Public Awareness and Training Working Group (PATWG) was established and chartered in August 2017. Since that time, a number of projects have been completed leading to the development of this plan. The PATWG has an established charter and has conducted a series of planning meetings. In addition, the group has conducted research on the topic and has engaged with a student team from IUPUI to develop an initial public awareness campaign in Indiana.

RESEARCH

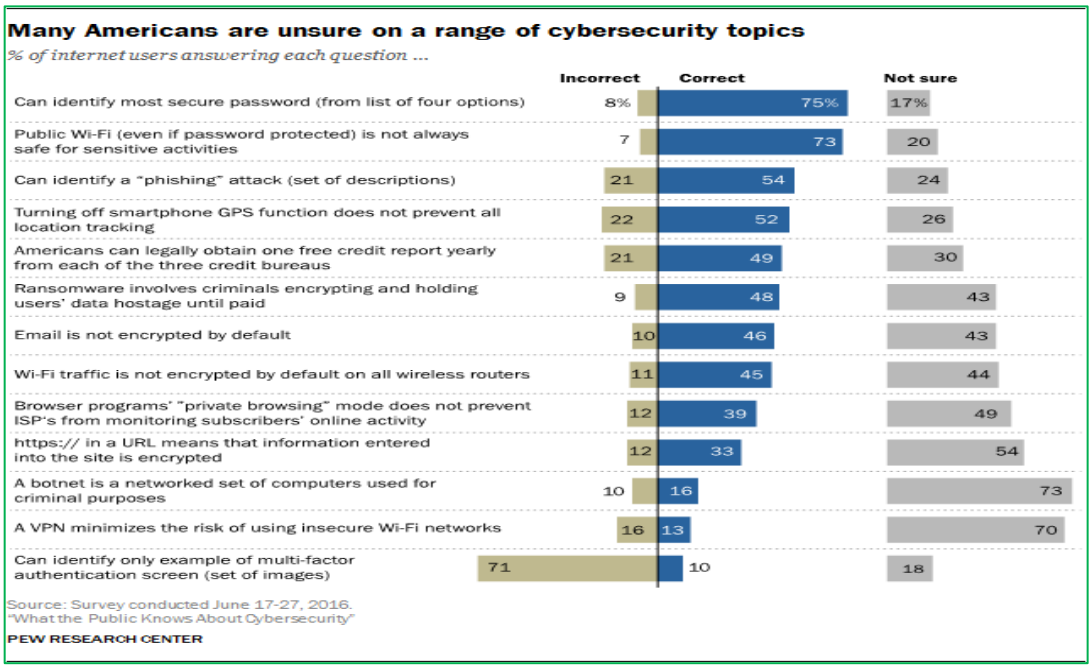
Summary

What research is available demonstrated that the greatest vulnerability is general lack of both awareness and knowledge among the general public on how best to protect themselves from cyberattacks. There is a significant public awareness and knowledge gap.

Research has established that there has essentially been no coordinated statewide effort to educate the general public about cybersecurity efforts. Individual industries and individual state agencies have conducted various programs focused generally in areas of their responsibility. The Indiana Attorney General has conducted a limited campaign focused primarily on identity theft, and IOT has extensive training opportunities available and has worked in a limited fashion to promote cybersecurity awareness. The Indiana Department of Revenue also has worked to educate taxpayers on fraud prevention over the past three years.

Specific Research Studies

1. PEW Research Center study: "What Americans Know About Cybersecurity." Conducted June 2016; Published March 2017. We anticipate that the findings from this survey of Americans can be generalized to Indiana residents.
    a. US nationwide survey of 1,055 adult internet users
    b. 13-question survey
    c. Observations:
        i. Typical respondent answered only 5 of 13 correctly!
        ii. Only 1 percent answered all 13 correctly!
        iii. Majority answered only 2 correctly!
        iv. Only 4 questions correctly answered by 50% or better



d. Operational Findings:
   i. Broad differences in knowledge by educational attainment
      – Significant differences between college and non-college respondents
   ii. Modest differences in knowledge by age
      – Younger = more knowledgeable
      – Older = less knowledgeable

2. "ACS Cybersecurity: Threats, Challenges, Opportunities." Australian Computer Society, Nov. 2016. This Australian association report provides a chapter dedicated to "Looking at the Road Ahead." It principally notes that there are few efforts worldwide to combat cybersecurity attacks. It notes that Japan has recently established and funded efforts to educate and train cybersecurity techniques in government, industry and with individuals. The report also identifies all the standard techniques for cybersecurity defense for businesses and industries. Perhaps most key in this report is the acknowledgement that the tools exist, we just need to educate and use them. As such, it places "education and awareness" as its number one priority out of five.

   a. Here are resources provided by this report (all Australian):
      - Australia's Cybersecurity Strategy - cybersecuritystrategy.dpmc.gov.au
      - Australian Center for Cyber Security - www.acsc.gov.au
      - Australian Computer Emergency Response Team (AusCERT) - www.auscert.org.au
      - Australian Cybercrime Online Reporting Network (ACORN) - www.acorn.gov.au
      - Australian Internet Security Initiative - www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative
      - Australian Signals Directorate – Top 4 Mitigation Strategies - www.asd.gov.au/infosec/mitigationstrategies.htm
      - Australian Signals Directorate – CyberSense Videos - www.asd.gov.au/videos/cybersense.htm
      - Australian Government – Stay Smart Online - www.staysmartonline.gov.au
      - ACCC – Scam Watch - www.scamwatch.gov.au

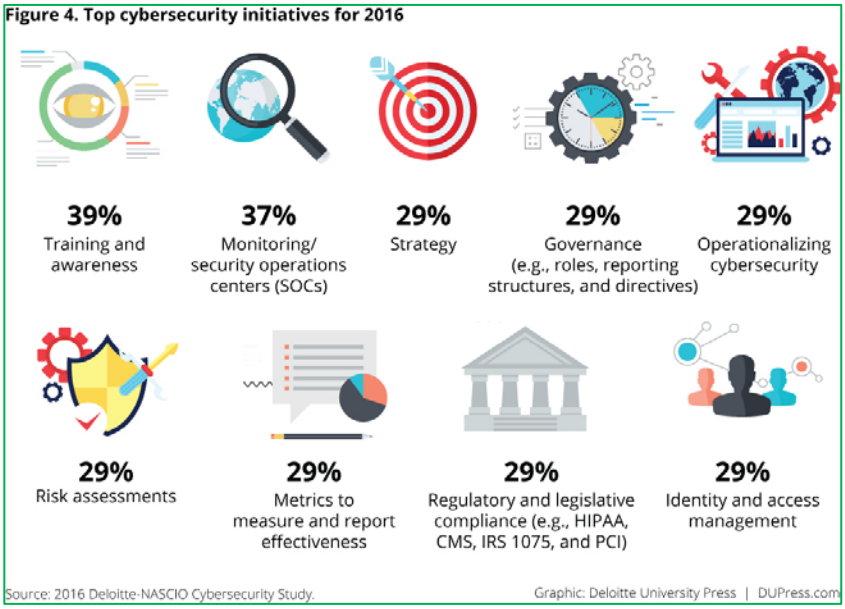
   b. Some key facts from the report:
      - The world economic forum's global risks 2015 report highlighted cyberattacks and threats as one of the most likely high-impact risks. In the United States, for example, cybercrime already costs an estimated $100 billion a year.
      - IOT Sensors and devices are expected to exceed mobile phones as the largest category of connected devices in 2018, growing at a 23% compound annual growth rate from 2015 to 2021.

- Cybersecurity is a business issue, not just a technology one. In a survey of close to 4,000 company directors in Australia, roughly only half reported to be cyber literate, and of co-directors, only 15 percent classed as cyber literate. There is a lack of knowledge about cybersecurity at the executive level in many businesses in Australia.
- There are 1,404 cybersecurity vendors in the world today. Vendors by country: USA 827; Israel 228; UK 76; India 41; Australia 15.
- Job advertisements for cybersecurity alone have grown 57% in the last 12 months according to jobs website Seek. Network security consultants were the 6th most advertised occupation on LinkedIn in 2015.

3. International Telecommunications Union (ITU) Global Cybersecurity Index 2017. This annual assessment of global (national and regional) cybersecurity efforts places the United States very high compared to most other regions and countries and observes that the National Governor's Association leads the way with its resource Center for State Cybersecurity.

4. Deliotte NASCIO Cybersecurity Study, Doug Robinson and Srini Subramanian, published September 20, 2016. This article examined state government efforts in cybersecurity protection and activity.

    a. One observation was that states are now taking a much more active role in cybersecurity defense. The figure below (extracted from the study) identifies the efforts now (2015) underway in comparison to other efforts in the cybersecurity arena. Note that Training and Awareness is the top area of priority and activity.



b. The study noted a positive trend in training of employees. All education and training trends are up across the board (between 2014 – 2016) except for third-party workforce.

Figure 22. Cybersecurity training trends for employees based on job role and function

States have made strides in increasing the breadth of security awareness training.

Provide required training to	Change from 2014 to 2016
Executives	↑
People handling sensitive information	↑
IT application developers and programmers	↑
System administrators	↑
IT infrastructure	↑
Business and program stakeholders	↑
General state workforce	↑
Third-party workforce (vendors, contractors, consultants, business partners)	↓

Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies. Graphic: Deloitte University Press | DUPress.com

5. "Cyber Security Awareness Campaigns: Why do they fail to change behavior?" draft working paper, Global Cyber Security Capability Center, July 2015.

a. This early research paper by academics in UK studies the nature of awareness and behavior change campaigns conducted to increase cybersecurity awareness and the adoption of new defensive behaviors.

b. Of particular note is the identification of six (6) "Essential Components for a Campaign:"

1. Communication. A significant part of a campaign is communication. This can be accomplished by collateral, internally distributed materials. These are things like newsletters, blogs, and other internal communications. Also, posters are a very crucial method of raising awareness. While some people believe they are old fashioned and outdated, they can be very effective when they are well designed.

2. Computer Based Training. CBT is the most omnipresent component of security awareness programs, as it is the most clearly accepted method of achieving compliance.

3. Events. Well-executed events bring the Security Awareness program, and the whole security effort for that matter, to life.

4. Security Portal. An internal security portal provides several functions. It provides a Knowledge base that can provide a huge return on investment with includes information on security related topics. It is also important to include information on home and personal security strategies, such as protecting children online and securing social media accounts.

5. Behavioral (sic) Testing and Teachable Moments. Phishing, USB drive drops, and Social Engineering tests require some care, but are important components to give your employees a "teachable moment."

6. Teaching New Skills Effectively. What looks like a lack of motivation is sometimes really a lack of ability (Patterson, Gremm, Maxfield, McMillan & Switzler, 2011). As teachers, security awareness professionals must break down complex goals in short, clear achievable steps.

c. The authors also identified seven (7) key factors that lead to campaign failure:

1. Not understanding what security awareness really is. Information must be provided in a way that relates to how people think and behave. There must be a personal association of how knowledge would impact their actions. There is also a difference in providing an individual information on a one-time basis, and delivering information in different formats over the course of time to effect change.

2. Compliance. In short, saying your awareness program is compliant does not necessarily equate to create the desired behaviors.

3. Illustrate that awareness is a unique discipline. A good security awareness professional will have good communication ability, be familiar with learning concepts, understand that awareness is more than a check the box activity, knowledge of a variety of techniques and awareness tools, and an understanding that there is a need for constant reinforcement of the desired behaviors.

4. Lack of engaging and appropriate materials.

5. Not collecting metrics. By collecting regular metrics, you can adjust your program to the measured effectiveness. By determining what is working and what is not, you can tailor future programs based upon lessons learned. The appropriate metrics also allow for the determination of which components are having the desired impact. They should be taken prior to starting any engagement effort, at least once during the engagement, and also post-engagement.

6. Unreasonable expectations. No security countermeasure will ever be completely successful at mitigating all incidents. There will always be a failure.

7. Arrange multiple training exercises. Focusing on a specific topic or threat does not offer the overall training needed.

d. Finally, the authors provide five (5) key factors that can lead to more sufficient awareness campaigns:

1. Awareness has to be professionally prepared and organized in order to work.

2. Causing feelings of fear to people is not an effective tactic, since it will put off people who can least afford to take risks. To make the internet accessible, risks should not be exaggerated.

3. Awareness alone is not enough. Usually all it does is catch attention.

4. Security education has to be more than providing information to people - it needs to be targeted, actionable, and doable. At the moment, what is correct behavior is far too difficult and complex. We need simple consistent rules of behavior that people can follow.

5. Once people are willing to change, training and feedback is needed to sustain them through the change period.

6. IUPUI student survey (convenience sample) conducted of Indiana residents, November 2017. General, small, self-selected sample of Indiana residents (mostly college students). Results generally reflect findings similar to the Pew Center Study.

7. The Working Group also undertook to discover existing resources within state government that could be use in a Cybersecurity campaign and what was available for cybersecurity training to both government personnel as well as industry employees and the general public. Those include:

- The Indiana Office of Technology (IOT) manages a state open website with extensive information and training opportunities for the general public.
    - Find it at https://www.in.gov/cybersecurity/2494.htm.
    - Additional tips at https://www.in.gov/cybersecurity/2571.html.
    - Additional training and education materials for the public are found at https://www.in.gov/cybersecurity/2533.htm and related pages.
- The Indiana Department of Homeland Security (IDHS) provides information on its website at https://www.in.gov/cybersecurity/2543.htm, including a cybersecurity fact sheet for businesses.

- Individual state agencies conduct awareness programs specific to their functions. For example, both the Indiana Department of Revenue (https://www.in.gov/dor/4794.htm) and the Indiana Attorney General (https://secure.in.gov/apps/ag/idtheftprevtoolkit/Login.aspx) conduct public identity theft education and awareness campaigns annually.

- IOT provides required cybersecurity training for all state employees annually. Some agencies test employees with phishing messages routinely, but this is not consistent across all agencies.

8. Initial, limited plan development.
   Opportunity provided the chance to engage with an IUPUI Public Relations Campaigns class and provide a team of students a chance at creating a campaign to increase cybersecurity awareness. Working with members of the working group, the student team identified two key publics to target with two key messages:

   - First, the general public was targeted for a general cybersecurity awareness campaign.
   - Second, high school students were targeted as a public to receive an awareness campaign focused on cybersecurity as a career field.

   The students created a draft campaign plan. This plan was used as a resource for the overarching master campaign plan represented in this document and, as such, has proved to be useful.

5-YEAR CAMPAIGN GOALS

- Phase 1: After one year:
  - Achieve awareness of cybersecurity protective measures to 50 percent of Hoosiers.
  - Achieve knowledge of cybersecurity protective measures to 25 percent of Hoosiers.
  - Achieve active Cybersecurity activities by Hoosiers to 15 percent.
  - Achieve 20 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
  - Achieve 10 percent awareness of cybersecurity as a career field among high school student.

- Phase 2: After three years:
  - Achieve 80 percent awareness of cybersecurity protective measures by Hoosiers.
  - Achieve knowledge of cybersecurity protective measures to 60 percent of Hoosiers.
  - Achieve 45 percent active cybersecurity protective measures by Hoosiers.
  - Achieve 50 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
  - Achieve 40 percent awareness of cybersecurity as a career field among high school student

- Phase 3: After five years:
  - Achieve 90 percent awareness of cybersecurity protective measures by Hoosiers.
  - Achieve knowledge of cybersecurity protective measures to 80 percent of Hoosiers.
  - Achieve 60 percent active cybersecurity protective measures by Hoosiers.
  - Achieve 75 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
  - Achieve 70 percent awareness of cybersecurity as a career field among high school student

PUBLICS

1. General Public (all Hoosiers).
    a. Baby Boomers and Traditionals, ages 54 to 72 and 72 and beyond.
    b. Gen X (ages 38-53) and Y (ages 23-37).
    c. Millennials (less than age 22)
    d. High School students (for careers goal).

2. State government employees.

3. Local Government employees.

4. Industry unique employees. Will be developed in Phase 2 of the working group's planning after close coordination with other committees and working groups.

PHASE 1 OUTCOMES AND EVALUATION

This campaign will use the questionnaire developed for the Pew Center Cybersecurity Awareness Study as a base for determining achievement of objectives. Those questions (awareness and knowledge points) are below:

1. Can identify most secure password (from list of four options).
2. Public Wi-Fi (even if password protected) is not always safe for sensitive activities.
3. Can identify a "phishing" attack (set of descriptions).
4. Turning off smartphone GPS function does not prevent all location tracking.
5. Americans can legally obtain one free credit report yearly from each of the three credit bureaus.
6. Ransomware involves criminals encrypting and holding users' data hostage until paid.
7. Email is not encrypted by default.
8. Wi-Fi traffic is not encrypted by default on all wireless routers.
9. Browser programs' "private browsing" mode does not prevent ISP's from monitoring subscribers' online activity.
10. Https:// in the URL means that information entered into the site is encrypted.
11. A botnet is a networked set of computers used for criminal purposes.
12. A VPN minimizes the risk of using insecurity Wi-Fi networks.
13. Can identify only example of multi-factor authentication screen (set of images).

Based on the PEW questionnaire, we identify via survey success at awareness and knowledgeability using the chart below.

Question	Aware	Knowledge	Action
Can identify	REQ	REQ	REQ
Public Wi-fi	REQ	REQ	REQ
Phishing	REQ	REQ	REQ
Turn off GPS	OPT	OPT	
Credit Reports	OPT	OPT	
Ransomware	OPT	OPT	
Encrypted email	OPT	REQ	REQ
Encrypted wi-fi	OPT	REQ	REQ
Private browsing	OPT	OPT	
Https	OPT	REQ	REQ
Botnet	OPT	OPT	
VPN	OPT	OPT	
Multi-factor Auth	OPT	REQ	REQ

1. **Awareness** equals correct answers to the 3 required questions and correct answers on at least 2 others.

2. **Knowledgeable** equals correct answers to the 7 required questions and at least one other.

3. **Action** will be measured via both survey and behavioral testing. To be considered "active" a respondent must correctly answer the Knowledge questions (reworded to ask them if they do those things as opposed to know those items) and also a small sample of the population will complete a behavioral lab test to confirm actual behavior

Evaluation at the end of Phase 1 will be conducted by a third-party research partner (university or private research firm) using a fully random sample survey of each population.

Evaluation results will be used to validate the target objectives for Phase 2.

PHASE 1
Phase 1 includes the initial year of the campaign from launch date (TBD) to one year later. It also includes an evaluation period at the end of the year. The evaluation data will be used to fine tune objectives for Phase 2.

PHASE 1 GOALS (after one year)

Goals:
1. Achieve awareness of cybersecurity protective measures to 50 percent of Hoosiers.
2. Achieve knowledge of cybersecurity protective measures to 25 percent of Hoosiers.
3. Achieve active Cybersecurity activities by Hoosiers to 15 percent.
4. Achieve 10 percent awareness of cybersecurity as a career field among high school student.
5. Achieve 20 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.

GOAL 1: ACHIEVE AWARENESS OF CYBERSECURITY PROTECTIVE MEASURES TO 50 PERCENT OF HOOSIERS.

Public: Baby Boomers/Traditionals, ages 54 and above.

OBJECTIVE 1-1: Achieve 50 percent awareness of cybersecurity protective measures among Indiana Baby Boomers/Traditionals one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy: This public is best reached via traditional media and secondarily via social media. Thus, the focus of our effort to reach this public will be earned media in newspapers, magazines and broadcast outlets in and around Indiana, as well as paid advertising and/or PSAs placed with the same media. The secondary approach will be social media, primarily Facebook. A tertiary approach will be to establish a speakers' bureau to support presentations to civic organizations around the state.

Message Strategy: Messaging should focus on building awareness and using the 13 key data points. Awareness is built by demonstrating a need. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Awareness messages such as: "Did You Know," How Can You…," "You are part of the Solution," and others similar are appropriate.

Tactics:

a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach.
b. Distribute monthly feature release on cybersecurity methods to all traditional print and broadcast media outlets in the state and contiguous counties of neighboring states.
c. Create PSAs and release monthly to radio outlets throughout the state matching the monthly feature release messaging.
d. Develop television media partners in each major market for cybersecurity messaging.
e. Create state-wide advertising campaign with monthly messaging releases to traditional print and broadcast media.
f. Develop special Facebook site to support social media messaging on this platform.
g. Develop a speakers' bureau of qualified speakers on individual cybersecurity protective measures and promote to civic organizations around the state.

Public: Gen X and Gen Y, ages 23-53.

OBJECTIVE 1-2: Achieve 50 percent awareness of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on building awareness and using the 13 key data points. Awareness is built by demonstrating a need. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Awareness messages such as: "Did You Know," How Can You…," "You are part of the Solution," and others similar are appropriate.

Tactics:

a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
c. Develop special Facebook site to support social media messaging on this platform.
d. Develop special Instagram site to support social media messaging on this platform.
e. Develop special Snapchat site to support social media messaging on this platform.
f. Develop special Twitter site to support social media messaging on this platform.
g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.

Public: Millennials (less than age 22)

OBJECTIVE 1-3: Achieve 50 percent awareness of cybersecurity protective measures among Indiana Millennials (less than age 22) one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on building awareness and using the 13 key data points. Awareness is built by demonstrating a need. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Awareness messages such as: "Did You Know," How Can You…," "You are part of the Solution," and others similar are appropriate.

Tactics:

a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
c. Develop special Facebook site to support social media messaging on this platform.
d. Develop special Instagram site to support social media messaging on this platform.
e. Develop special Snapchat site to support social media messaging on this platform.
f. Develop special Twitter site to support social media messaging on this platform.
g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.

Public: State government employees

Objective 1-4: Achieve 50 percent awareness of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy: This public is already reached very effectively by state-mandated cybersecurity training and will require little to no effort during this campaign.

Message Strategy: Messaging should focus on building awareness and using the 13 key data points. Awareness is built by demonstrating a need. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Awareness messages such as: "Did You Know," How Can You…," "You are part of the Solution," and others similar are appropriate.

Tactics**:**
Continue current activities via IOT.

Public: Local government employees

Objective 1-5: Achieve 50 percent awareness of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy**:** Strategies to reach other publics will also reach this public. However, this public is especially vulnerable and will need special approaches and messaging via a direct email campaign. Training opportunities will be developed (ICW state programs) to bring cybersecurity training to this public.

Message Strategy: Messaging should focus on building awareness and using the 13 key data points. Awareness is built by demonstrating a need. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Awareness messages such as: "Did You Know," How Can You…," "You are part of the Solution," and others similar are appropriate.

Special Tactics:

a. Develop a training opportunity for all local government employees that emulates or duplicates that required of state employees.
b. Require all local government employees to take the training annually.
c. Provide monthly communication to all local government entities promoting cybersecurity protective measures both on the job and in their personal lives. Communication should include the following:
    1. Monthly email messages
    2. Monthly Print feature stories
    3. Monthly website postings for intranets

GOAL 2. ACHIEVE KNOWLEDGE OF CYBERSECURITY PROTECTIVE MEASURES TO 25 PERCENT OF HOOSIERS.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 2-1: Achieve 25 percent knowledge of cybersecurity protective measures among Indiana Baby Boomers/Traditionals one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy: This public is best reached via traditional media and secondarily via social media. Thus, the focus of our effort to reach this public will be earned media in newspapers, magazines and broadcast outlets in and around Indiana, as well as paid advertising and/or PSAs placed with the same media. The secondary approach will be social media, primarily Facebook. A tertiary approach will be to establish a speakers' bureau to support presentations to civic organizations around the state.

Message Strategy: Messaging should focus on building knowledge and using the 13 key data points. Knowledge is built by providing constant and consistent information. As such, an informative strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Knowledge messages such as: "Did You Know," How Can You…," "You are part of the Solution," "You can…," and others similar are appropriate.

Tactics:

a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach.
b. Distribute monthly feature release on cybersecurity methods to all traditional print and broadcast media outlets in the state and contiguous counties of neighboring states.
c. Create PSAs and release monthly to radio outlets throughout the state matching the monthly feature release messaging.
d. Develop television media partners in each major market for cybersecurity messaging.
e. Create state-wide advertising campaign with monthly messaging releases to traditional print and broadcast media.
f. Develop special Facebook site to support social media messaging on this platform.
g. Develop a speakers' bureau of qualified speakers on individual cybersecurity protective measures and promote to civic organizations around the state.

Public: Gen X and Gen Y, ages 23-53

Objective 2-2: Achieve 25 percent knowledge of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on building knowledge and using the 13 key data points. Knowledge is built by providing constant and consistent information. As such, an informative strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Knowledge messages such as: "Did You Know," How Can You…," "You are part of the Solution," "You can…," and others similar are appropriate.

Tactics:

a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
c. Develop special Facebook site to support social media messaging on this platform.
d. Develop special Instagram site to support social media messaging on this platform.
e. Develop special Snapchat site to support social media messaging on this platform.
f. Develop special Twitter site to support social media messaging on this platform.
g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.

Public: Millennials (less than age 22)

Objective 2-3: Achieve 25 percent knowledge of cybersecurity protective e measures among Indiana Millennials (less than age 22) one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on building knowledge and using the 13 key data points. Knowledge is built by providing constant and consistent information. As such, an informative strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Knowledge messages such as: "Did You Know," How Can You…," "You are part of the Solution," "You can…," and others similar are appropriate.

Tactics:

a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
c. Develop special Facebook site to support social media messaging on this platform.
d. Develop special Instagram site to support social media messaging on this platform.
e. Develop special Snapchat site to support social media messaging on this platform.
f. Develop special Twitter site to support social media messaging on this platform.
g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.

Public: State government employees

Objective 2-4: Achieve 25 percent knowledge of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy: This public is already reached very effectively by state-mandated cybersecurity training and will require little to no effort during this campaign.

Message Strategy: Messaging should focus on building knowledge and using the 13 key data points. Knowledge is built by providing constant and consistent information. As such, an informative strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Knowledge messages such as: "Did You Know," How Can You…," "You are part of the Solution," "You can…," and others similar are appropriate.

Tactics:
Continue current activities via IOT.

Public: Local government employees

Objective 2-5: Achieve 25 percent knowledge of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy: Strategies to reach other publics will also reach this public. However, this public is especially vulnerable and will need special approaches and messaging via a direct email campaign. Training opportunities will be developed (ICW state programs) to bring cybersecurity training to this public.

Message Strategy: Messaging should focus on building knowledge and using the 13 key data points. Knowledge is built by providing constant and consistent information. As such, an informative strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Knowledge messages such as: "Did You Know," How Can You…," "You are part of the Solution," "You can…," and others similar are appropriate.

Special Tactics:

a. Develop a training opportunity for all local government employees that emulates or duplicates that required of state employees.
b. Require all local government employees to take the training annually.
c. Provide monthly communication to all local government entities promoting cybersecurity protective measures both on the job and in their personal lives. Communication should include the following:
    1. Monthly email messages
    2. Monthly Print feature stories
    3. Monthly website postings for intranets

GOAL 3. ACHIEVE 15 PERCENT OF HOOSIERS ACTIVE IN CYBERSECURITY ACTIVITIES.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 3-1: Achieve 15 percent active personal cybersecurity actions among Indiana Boomers/Traditionals one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy: This public is best reached via traditional media and secondarily via social media. Thus, the focus of our effort to reach this public will be earned media in newspapers, magazines and broadcast outlets in and around Indiana, as well as paid advertising and/or PSAs placed with the same media. The secondary approach will be social media, primarily Facebook. A tertiary approach will be to establish a speakers' bureau to support presentations to civic organizations around the state.

Message Strategy: Messaging should focus on promoting action using the 13 key behaviors identified in the Pew Study. Action is built by providing constant and consistent persuasive and action messaging. These should always include a "call to action" step. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Action messages such as: "To be part of the solution…," "How Can You…," "You can protect yourself…," "You can help by…," and others similar are appropriate.

Tactics:

a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach.
b. Distribute monthly feature release on cybersecurity methods to all traditional print and broadcast media outlets in the state and contiguous counties of neighboring states.
c. Create PSAs and release monthly to radio outlets throughout the state matching the monthly feature release messaging.
d. Develop television media partners in each major market for cybersecurity messaging.
e. Create state-wide advertising campaign with monthly messaging releases to traditional print and broadcast media.
f. Develop special Facebook site to support social media messaging on this platform.
g. Develop a speakers' bureau of qualified speakers on individual cybersecurity protective measures and promote to civic organizations around the state.

Public: Gen X (ages 38-53) and Y (ages 23-37).

Objective 3-2: Achieve 15 percent active personal cybersecurity actions among Indiana Generation X'ers one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on promoting action using the 13 key behaviors identified in the Pew Study. Action is built by providing constant and consistent persuasive and action messaging. These should always include a "call to action" step. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Action messages such as: "To be part of the solution…," "How Can You…," "You can protect yourself…," "You can help by…," and others similar are appropriate.

Tactics:

a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
c. Develop special Facebook site to support social media messaging on this platform.
d. Develop special Instagram site to support social media messaging on this platform.
e. Develop special Snapchat site to support social media messaging on this platform.
f. Develop special Twitter site to support social media messaging on this platform.
g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.

Public: Millennials (less than age 22)

Objective 3-3: Achieve 15 percent active personal cybersecurity actions among Indiana Millennials one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook.

Message Strategy: Messaging should focus on promoting action using the 13 key behaviors identified in the Pew Study. Action is built by providing constant and consistent persuasive and action messaging. These should always include a "call to action" step. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Action messages such as: "To be part of the solution…," "How Can You…," "You can protect yourself…," "You can help by…," and others similar are appropriate.

Tactics:

a. Develop special website with key cybersecurity protective measure information for individuals that can be used in conjunction with media outreach. Site should host detailed information, feature stories, etc. that can support a social media campaign.
b. Create state-wide social media advertising campaign with consistent monthly messaging releases to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
c. Develop special Facebook site to support social media messaging on this platform.
d. Develop special Instagram site to support social media messaging on this platform.
e. Develop special Snapchat site to support social media messaging on this platform.
f. Develop special Twitter site to support social media messaging on this platform.
g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity protective measures and features that support the need for individual protection.

Public: Indiana state government employee

Objective 3-4: Achieve 15 percent active cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Active = This public can positively answer 5 of 7 key personal protection questions/tactics identified in the evaluation table.

Strategy: This public is already reached very effectively by state-mandated cybersecurity training and will require little to no effort during this campaign.

Tactics:
Continue current activities via IOT.

Public: Local government employees

Objective 3-5: Achieve 15 percent active cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is can positively answer 5 of 7 key personal protection questions/tactics in the evaluation table.

Strategy: Strategies to reach other publics will also reach this public. However, this public is especially vulnerable and will need special approaches and messaging via a direct email campaign. Training opportunities will be developed (ICW state programs) to bring cybersecurity training to this public.

Message Strategy: Messaging should focus on promoting action using the 13 key behaviors identified in the Pew Study. Action is built by providing constant and consistent persuasive and action messaging. These should always include a "call to action" step. As such, a persuasive strategy is appropriate. In addition, research indicates that positive message framing techniques are most effective. Action messages such as: "To be part of the solution…," "How Can You…," "You can protect yourself…," "You can help by…," and others similar are appropriate.

Special Tactics:

a. Develop a training opportunity for all local government employees that emulates or duplicates that required of state employees.
b. Require all local government employees to take the training annually.
c. Provide monthly communication to all local government entities promoting cybersecurity protective measures both on the job and in their personal lives. Communication should include the following:
    1. Monthly email messages
    2. Monthly Print feature stories
    3. Monthly website postings for intranets

GOAL 4. ACHIEVE 10 PERCENT AWARENESS OF CYBERSECURITY AS A CAREER FIELD AMONG HIGH SCHOOL STUDENTS.

Public: Indiana high school students

Objective 4-1: Achieve 10 percent awareness that cybersecurity is a viable career field among Indiana high school students within one year after campaign launch.

Awareness = This public can answer 3 of 8 questions in a survey about viable cybersecurity careers in Indiana. (An awareness test for cybersecurity careers will be created for evaluation purposes.)

Strategy: This public is reachable almost exclusively via social media and that will be the primary approach. The effort will include social media placements in key platforms, including Facebook, Instagram, Snapchat, and Twitter as well as paid placements in Facebook. A secondary effort will approach key influencers like guidance counselors and technology teachers via conferences, direct mail, and the provision of collateral materials that promote the career field and provide information about its various elements and higher education opportunities and scholarships.

Message Strategy: Awareness is built initially via both informative and persuasive messages framed positively. To build awareness, messaging should include a focus on informing students about cybersecurity opportunities and persuading them to think positively about cybersecurity as a potential career field and field of study. Thus, messages should include statistics about open opportunities, salary information, educational opportunities, career advancement, scholarship opportunities, etc. Additionally, persuasive messaging should also be used to engage students. Thus, success stories and testimonials are appropriate.

Tactics:

a. Develop special website with key Information about cybersecurity career opportunities for high school that can be used in conjunction with media outreach. Site should host detailed information, feature stories, in-state education opportunities, scholarship opportunities, etc. that can support a social media campaign.
b. Create state-wide social media advertising campaign with a focus on opportunities for careers in cybersecurity to large-population center media. Specific target should be Facebooks, Instagram and Twitter.
c. Develop special Facebook site to support social media careers messaging on this platform.
d. Develop special Instagram site to support social media careers messaging on this platform.
e. Develop special Snapchat site to support social media careers messaging on this platform.
f. Develop special Twitter site to support social media careers messaging on this platform.

g. Distribute content to social media sites on a consistent basis. Content should focus on cybersecurity career and education and features that highlight those opportunities.
h. Create an outreach program for technology instructors/teachers in high schools that provides them information to share with students about cybersecurity careers and educational opportunities.
    1. Working with industry groups, create a cybersecurity speakers' bureau of cybersecurity professionals who can speak at high schools around the state.
    2. Promote the speakers' bureau to high school technology teachers.
    3. Create key collateral materials including a brochure, fact sheets, etc. that can be provided to technology teachers and speakers'.
    4. Work with university programs that offer cybersecurity education and training to integrate their efforts in the campaign.
    5. Use direct mail (printed) and email to communicate with technology teachers the opportunities for both careers and speakers'. Message at least monthly during school year.

GOAL 5. ACHIEVE 20 PERCENT AWARENESS OF STATEWIDE CYBERSECURITY PROTECTIVE ACTIVITIES BY GOVERNMENT AND INDUSTRY AMONG HOOSIERS.

Public: all Hoosiers

Objective 5-1: Achieve 20 percent awareness among all Hoosiers about the activities of the state to improve cybersecurity protection in Indiana within the first year of the campaign.

Awareness = This public can answer 3 of 7 questions on a survey that identifies specific actions being taken to improve cybersecurity in Indiana (Evaluation tool to be created.).

Strategy: This very broad public is best reached via traditional media and secondarily via social media. Thus, the focus of our effort to reach this public will be earned media in newspapers, magazines and broadcast outlets in and around Indiana. The secondary approach will be social media, primarily Facebook and LinkedIn. A tertiary approach will be to establish a speakers' bureau to support presentations to civic organizations around the state.

Message Strategy:

Tactics:

a. Establish a key public affairs position in the governor's office responsible for coordinating public information about cybersecurity state-wide, including overall coordination with Council and key departments (such as IOT, IDHS, State Police, others).
b. Conduct a new conference upon completion of initial Cybersecurity Plan featuring the Governor and key Council leadership – especially industry partners**.** Support with news release and media kit. Consider this an annual event.
c. Distribute monthly news release to all state media with key activities conducted during past month on a monthly basis.
d. Conduct an annual cybersecurity conference and publicize heavily.
e. Offer cybersecurity interviews routinely (at least quarterly) to key media, including business media, public affairs television shows, editorial boards of key newspapers, etc.

KEY OVERALL MESSAGES FOR PHASE 1

- Cybersecurity awareness is everyone's business.
- Cybersecurity knowledge is important to protect individuals and critical infrastructure.
- Cybersecurity activities are important to the defense of our identities, our computers, and our critical infrastructure networks.
- Cybersecurity training is free and available.
- Cybersecurity is a profession (targeted to high school students).
- The Cybersecurity Council's activities in helping defend Indiana from cyberattack. (this includes efforts by industries and sectors in the state via the C/WGs)
- Additional, very specific key messages:
    1. Effective and secure passwords are at least x characters long and include letters, numbers and symbols.
    2. Public Wi-Fi (even if password protected) is not always safe for sensitive activities.
    3. A "phishing" attack is an effort to gain access to your personal information by getting you to reveal your logon and password information.
    4. Turning off smartphone GPS function does not prevent all location tracking.
    5. Americans can legally obtain one free credit report yearly from each of the three credit bureaus.
    6. Ransomware involves criminals encrypting and holding users' data hostage until paid.
    7. Email is not encrypted by default.
    8. Wi-Fi traffic is not encrypted by default on all wireless routers.
    9. Browser programs' "private browsing" mode does not prevent ISP's from monitoring subscribers' online activity.
    10. Https:// in the URL means that information entered into the site is encrypted.
    11. A botnet is a networked set of computers used for criminal purposes.
    12. A VPN minimizes the risk of using insecurity Wi-Fi networks.
    13. Using multi-factor authentication significantly enhances your personal online security.

GOALS PHASE 2: AFTER THREE YEARS (YEAR 2 & 3 OF THE CAMPAIGN):

Note: These outcomes, and the development of their appropriate strategies and tactics, will be updated using data/results from the evaluation of Phase 1 goals and objectives.

PHASE 2 GOALS

1. Achieve 80 percent awareness of cybersecurity protective measures by Hoosiers.
2. Achieve knowledge of cybersecurity protective measures to 60 percent of Hoosiers.
3. Achieve 45 percent active cybersecurity protective measures by Hoosiers.
4. Achieve 50 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
5. Achieve 40 percent awareness of cybersecurity as a career field among high school student

PHASE 2 OUTCOMES AND EVALUATION

This campaign will use the questionnaire developed for the Pew Center Cybersecurity Awareness Study as a base for determining achievement of objectives. Those questions (awareness and knowledge points) are below:

1. Can identify most secure password (from list of four options).
2. Public Wi-Fi (even if password protected) is not always safe for sensitive activities.
3. Can identify a "phishing" attack (set of descriptions).
4. Turning off smartphone GPS function does not prevent all location tracking.
5. Americans can legally obtain one free credit report yearly from each of the three credit bureaus.
6. Ransomware involves criminals encrypting and holding users' data hostage until paid.
7. Email is not encrypted by default.
8. Wi-Fi traffic is not encrypted by default on all wireless routers.
9. Browser programs' "private browsing" mode does not prevent ISP's from monitoring subscribers' online activity.
10. Https:// in the URL means that information entered into the site is encrypted.
11. A botnet is a networked set of computers used for criminal purposes.
12. A VPN minimizes the risk of using insecurity Wi-Fi networks.
13. Can identify only example of multi-factor authentication screen (set of images).

Based on the PEW questionnaire, we identify via survey success at awareness and knowledgeability using the chart below.

Question	Aware	Knowledge	Action
Can identify	REQ	REQ	REQ
Public Wi-fi	REQ	REQ	REQ
Phishing	REQ	REQ	REQ
Turn off GPS	OPT	OPT	OPT
Credit Reports	REQ	REQ	REQ
Ransomware	REQ	REQ	REQ
Encrypted email	OPT	REQ	REQ
Encrypted wi-fi	OPT	REQ	REQ
Private browsing	OPT	OPT	OPT
Https	OPT	REQ	REQ
Botnet	OPT	OPT	OPT
VPN	OPT	REQ	REQ
Multi-factor Auth	REQ	REQ	REQ

4. **Awareness** equals correct answers to the 6 required questions and correct answers on at least 2 others.

5. **Knowledgeable** equals correct answers to the 10 required questions and at least one other.

6. **Action** will be measured via both survey and behavioral testing. To be considered "active" a respondent must correctly answer the Knowledge questions (reworded to ask them if they do those things as opposed to know those items) and also a small sample of the population will complete a behavioral lab test to confirm actual behavior

Evaluation at the end of Phase 2 will be conducted by a third-party research partner (university or private research firm) using a fully random sample survey of each population.

Evaluation results will be used to validate the target objectives for Phase 3.

GOAL 1. ACHIEVE 80 PERCENT AWARENESS OF CYBERSECURITY PROTECTIVE MEASURES BY HOOSIERS.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 1-1: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Baby Boomers/Traditionals three years after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy:

Tactics:

Public: 2-Gen X and Gen Y, ages 23-53.

Objective 1-2: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) three years after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy:

Tactics:

Public: Millennials (less than age 22)

Objective 1-3: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Millennials (less than age 22) three years after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy:

Tactics:

Public: State government employees

Objective 1-4: Achieve 80 percent awareness of cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy:

Tactics:

Public: Local government employees

Objective 1-5: Achieve 80 percent awareness of cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Strategy:

Tactics:

GOAL 2. ACHIEVE KNOWLEDGE OF CYBERSECURITY PROTECTIVE MEASURES TO 60 PERCENT OF HOOSIERS.

Public: Traditionals

Objective 2-1: Achieve 60 percent knowledge of cybersecurity protective measures among Indiana Baby Boomers/Traditionals three years after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy:

Tactics:

Public: Gen X and Y

Objective 2-2: Achieve 60 percent knowledge of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) three years after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy:

Tactics:

Public: Millennials

Objective 2-3: Achieve 60 percent knowledge of cybersecurity protective e measures among Indiana Millennials (less than age 22) three years after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy:

Tactics:

Public: State government employees

Objective 2-4: Achieve 60 percent knowledge of cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy**:**

Tactics**:**

Public: Local government employees

Objective 2-5: Achieve 60 percent knowledge of cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Strategy:

Tactics:

GOAL 3. ACHIEVE 45 PERCENT ACTIVE CYBERSECURITY PROTECTIVE MEASURES BY HOOSIERS.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 3-1: Achieve 45 percent active personal cybersecurity actions among Indiana Boomers/Traditionals three years after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy:

Tactics:

Public: Gen X (ages 38-53) and Y (ages 23-37).

Objective 3-2: Achieve 45 percent active personal cybersecurity actions among Indiana Generation X'ers three years after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy:

Tactics:

Public: Millennials (less than age 22)

Objective 3-3: Achieve 45 percent active personal cybersecurity actions among Indiana Millennials three years after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Strategy:

Tactics:

Public: state government employees

Objective 3-4: Achieve 45 percent active cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Active = This public can positively answer 5 of 7 key personal protection questions/tactics identified in the evaluation table.

Strategy:

Tactics:

Public: Local government employees

Objective 3-5: Achieve 45 percent active cybersecurity protective measures among Indiana state government employees three years after campaign launch.

Awareness = This public is can positively answer 5 of 7 key personal protection questions/tactics in the evaluation table.

Strategy:

Tactics:

GOAL 4. ACHIEVE 40 PERCENT AWARENESS OF CYBERSECURITY AS A CAREER FIELD AMONG HIGH SCHOOL STUDENT

Public: Indiana High School students

Objective 4-1: Achieve 40 percent awareness that cybersecurity is a viable career field among Indiana high school students within one year after campaign launch.

Awareness = This public can answer 3 of 8 questions in a survey about viable cybersecurity careers in Indiana. (Create awareness test for cybersecurity careers. Will recruit some help here.)

GOAL 5. ACHIEVE 50 PERCENT AWARENESS OF STATEWIDE CYBERSECURITY PROTECTIVE ACTIVITIES BY GOVERNMENT AND INDUSTRY AMONG HOOSIERS.

Public: All Hoosiers

Objective 5-1: Achieve 50 percent awareness among all Hoosiers about the activities of the state to improve cybersecurity protection in Indiana within the first year of the campaign.

Awareness = This public can answer 4 of 7 questions on a survey that identifies specific actions being taken to improve cybersecurity in Indiana (evaluation tool to be created).

Strategy:
Tactics:

GOALS PHASE 3: AFTER FIVE YEARS:

Note: These outcomes, and the development of their appropriate strategies and tactics, will be updated using data/results from the evaluation of Phase 2 goals and objectives (at the end of year three of the campaign).

GOALS

1. Achieve 90 percent awareness of cybersecurity protective measures by Hoosiers.
2. Achieve knowledge of cybersecurity protective measures to 80 percent of Hoosiers.
3. Achieve 60 percent active cybersecurity protective measures by Hoosiers.
4. Achieve 75 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.
5. Achieve 70 percent awareness of cybersecurity as a career field among high school student

PHASE 3 OUTCOMES AND EVALUATION

This campaign will use the questionnaire developed for the Pew Center Cybersecurity Awareness Study as a base for determining achievement of objectives. Those questions (awareness and knowledge points) are below:

1. Can identify most secure password (from list of four options).
2. Public Wi-Fi (even if password protected) is not always safe for sensitive activities.
3. Can identify a "phishing" attack (set of descriptions).
4. Turning off smartphone GPS function does not prevent all location tracking.
5. Americans can legally obtain one free credit report yearly from each of the three credit bureaus.
6. Ransomware involves criminals encrypting and holding users' data hostage until paid.
7. Email is not encrypted by default.
8. Wi-Fi traffic is not encrypted by default on all wireless routers.
9. Browser programs' "private browsing" mode does not prevent ISP's from monitoring subscribers' online activity.
10. Https:// in the URL means that information entered into the site is encrypted.
11. A botnet is a networked set of computers used for criminal purposes.
12. A VPN minimizes the risk of using insecurity Wi-Fi networks.
13. Can identify only example of multi-factor authentication screen (set of images).

Based on the PEW questionnaire, we identify via survey success at awareness and knowledgeability using the chart below.

Question	Aware	Knowledge	Action
Can identify	REQ	REQ	REQ
Public Wi-fi	REQ	REQ	REQ
Phishing	REQ	REQ	REQ
Turn off GPS	REQ	REQ	REQ
Credit Reports	REQ	REQ	REQ
Ransomware	REQ	REQ	REQ
Encrypted email	OPT	REQ	REQ
Encrypted wi-fi	OPT	REQ	REQ
Private browsing	OPT	REQ	REQ
Https	OPT	REQ	REQ
Botnet	OPT	REQ	REQ
VPN	REQ	REQ	REQ
Multi-factor Auth	REQ	REQ	REQ

7. **Awareness** equals correct answers to the 8 required questions and correct answers on at least 1 other.

8. **Knowledgeable** equals correct answers to the 10 required questions and at least two others.

9. **Action** will be measured via both survey and behavioral testing. To be considered "active" a respondent must correctly answer the Knowledge questions (reworded to ask them if they do those things as opposed to know those items) and also a small sample of the population will complete a behavioral lab test to confirm actual behavior

Evaluation at the end of Phase 3 will be conducted by a third-party research partner (university or private research firm) using a fully random sample survey of each population.

Goal 1. Achieve 90 percent awareness of cybersecurity protective measures by Hoosiers.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 1-1: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Baby Boomers/Traditionals one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Public: 2-Gen X and Gen Y, ages 23-53.

Objective 1-2: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Public: Millennials (less than age 22)

Objective 1-3: Achieve 80 percent awareness of cybersecurity protective measures among Indiana Millennials (less than age 22) one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Public: State government employees

Objective 1-4: Achieve 80 percent awareness of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Public: Local government employees

Objective 1-5: Achieve 80 percent awareness of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is aware of the first 3 key personal protection questions/tactics and at least 2 others on the list.

Goal 2. Achieve knowledge of cybersecurity protective measures to 80 percent of Hoosiers.

Public: Baby Boomers/Traditionals

Objective 2-1: Achieve 80 percent knowledge of cybersecurity protective measures among Indiana Baby Boomers/Traditionals one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Public: Gen Xers and Gen Yers

Objective 2-2: Achieve 80 percent knowledge of cybersecurity protective measures among Indiana Gen Xers and Gen Yers (ages 23-53) one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Public: Millennials

Objective 2-3: Achieve 80 percent knowledge of cybersecurity protective e measures among Indiana Millennials (less than age 22) one year after campaign launch.

Knowledge = This public is aware of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Public: State government employees

Objective 2-4: Achieve 80 percent knowledge of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Public: Local government employees

Objective 2-5: Achieve 80 percent knowledge of cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is knowledgeable of the first 7 key personal protection questions/tactics and at least 1 other on the list.

Goal 3. Achieve 60 percent active cybersecurity protective measures by Hoosiers.

Public: Baby Boomers/Traditionals, ages 54 and above.

Objective 3-1: Achieve 60 percent active personal cybersecurity actions among Indiana Boomers/Traditionals one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Public: Gen X (ages 38-53) and Y (ages 23-37).

Objective 3-2: Achieve 60 percent active personal cybersecurity actions among Indiana Generation X'ers one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Public: Millennials (less than age 22)

Objective 3-3: Achieve 60 percent active personal cybersecurity actions among Indiana Millennials one year after campaign launch.

Active = Public can positively answer 5 of 7 of the key personal protection questions/actions identified in the evaluation table.

Public: Indiana state government employees

Objective 3-4: Achieve 60 percent active cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Active = This public can positively answer 5 of 7 key personal protection questions/tactics identified in the evaluation table.

Public: Local government employees

Objective 3-5: Achieve 60 percent active cybersecurity protective measures among Indiana state government employees one year after campaign launch.

Awareness = This public is can positively answer 5 of 7 key personal protection questions/tactics in the evaluation table.

Goal 4. Achieve 70 percent awareness of cybersecurity as a career field among high school students.

Public**:** Indiana high school students

Objective 4-1: Achieve 70 percent awareness that cybersecurity is a viable career field among Indiana high school students within one year after campaign launch.

Awareness = This public can answer 3 of 8 questions in a survey about viable cybersecurity careers in Indiana. (Create awareness test for cybersecurity careers. Will recruit some help here.)

Goal 5. Achieve 75 percent awareness of statewide cybersecurity protective activities by government and industry among Hoosiers.

Public: all Hoosiers

Objective 5-1: Achieve 75 percent awareness among all Hoosiers about the activities of the state to improve cybersecurity protection in Indiana within the first year of the campaign.

Awareness = This public can answer 5 of 7 questions on a survey that identifies specific actions being taken to improve cybersecurity in Indiana (evaluation tool to be created.).

Outline Budget

Cybersecurity Public Awareness Plan: Phase 1 (first year) only
Activities drawn from Tactics for Phase 1 Goals and Objectives

This outline budget is applicable to the Phase 1 activities identified in this plan. It is based on best estimates for all of the strategies and tactics recommended. It is also expected, however, that this budget will be fine-tuned as agents are assigned for plan execution, and as selected tactical activities are either selected or rejected in the normal process of plan execution.

It assumes that one or more persons be hired to manage the campaign overall with either assistance from multiple state agencies, and/or with assistance from a third-party vendor – an advertising or public relations firm.

It is also important to note that this budget does not address training management nor the cost of obtaining and delivering cybersecurity training to local government employees or others.

Additionally, while we have recommended the Cybersecurity program be properly "branded," the cost of that effort is not included in this budget.

Activity	Description	Agent	Cost	Notes
Cybersecurity Public Relations Director	Per recommendation, hire a senior public relations professional to take overall responsibility for the campaign and also serve as overall spokesperson on cybersecurity issues.	New Hire; locate in Governor's office with appropriate directive authority.	$119,000	Estimated based on a hire at $85,000 plus benefits (@40%).
Website	Develop and maintain a website designed specifically for the public to provide information on cybersecurity protective measures and education/training opportunities	State: IOT (continue and expand current site; rebrand away from IOT	$0	Assume this rebranding and build/maintain can be accomplished in-house using collective assets
Earned Media	Monthly feature release on cybersecurity methods to print and broadcast media	CS PR Director	$0	In-house activity
PSAs	Create and distribute monthly PSAs to radio outlets around the state matching news release feature messages.	CS PR Director	$12,000*	This may be handled in-house if technology and distribution can be managed. Otherwise, contract to external agency. $1,000 per month.
Media Partners	Develop relationship with at least one television partner in each major market to help distribute information on cybersecurity	CS PR Director	$0	Expect this activity can be handled in-house. Results will vary as will actual activities.

Activity	Description	Agent	Cost	Notes
Advertising Campaign	Create state-wide advertising campaign (print, radio, television, social media) to deliver cybersecurity messages on a consistent monthly basis.	External agency supervised by CS PR Director	$5,000 $1,500 $10,000 Total: $143,000	Initial campaign development Monthly creative Monthly ad buy
Social media	Create new Facebook, Instagram, Twitter, Snapchat, LinkedIn sites/pages focused on Cybersecurity and branded appropriately.	In house managed by CS PR Director and executed via identified agencies in coordination.	$0	In house
Speakers' Bureau	Develop, promote and maintain a speakers' bureau to provide speakers to civic and other organizations on Cybersecurity.	Directed by CS PR Director using a volunteer state agency to manage. Alternative: hire entry level PR professional to manage. Use qualitied volunteers for speakers.	$0 $42,000 $12,000	Development and maintenance. Alt: PR Coordinator: $30,000 plus benefits. Note: if hiring, this coordinator also can assume other cybersecurity communication responsibilities for this program reducing reliance on other agencies who would perform these duties as collateral responsibility. Travel and expenses for speakers at $1,000 monthly
Local Government Training Program	Develop and support local government employee training program meeting the same standards as state government employees.	Managed locally and operated via IOT Training.	$???	
Local government direct email	Consistent with features and web materials, promotion monthly via email directly to all local government employees`	CS PR Director ICW local governments	$0	In-house; will require close coordination with local government entities. Probably simplest to provide copy to key contacts for redistribution.
Local government feature stories and web postings	Materials produced and provided to local governments for use and promotion via email.	Direction: CS PR Director Action: Shared responsibility with key agencies	$0	Assumed that materials produced for state distribution can be repackaged for local government distribution.
Total (low estimate)			**$286,000**	Local training costs not included
Total (high estimate)	Recommended		**$328,000**	Local training costs not included

Activity	Description	Agent	Cost	Notes
Option:	Understanding that this campaign may need to be implemented earlier than a solid budget can be allocated, one way to reduce the cost is to defer the paid advertising program to Phase 2 (second two years). That would save $143,000 this initial first-year budget.		**$185,000**	Local training costs not included
Note:	Training management and coordination			This budget does not include provision for a central training manager to coordinate available training assets for delivery to various publics, including local government employees.

ITU
Cybersecurity Index

2017

ITU-D

Global Cybersecurity Index (GCI) 2017

Global Cybersecurity Index 2017

Acknowledgments

This report has been produced by the International Telecommunication Union (ITU) with the support of Michael Minges. The Cybersecurity Team of the ITU would like to express its appreciation to Dr. Sherif Hashem (NTRA Egypt), Michaela Saisanna and Hedvig Norlen (Joint Research Centre of the European Commission) as well as the Rapporteurs of the Study Group 2 Question 3 Rozalin Al-Balushi (Oman) and Eliot Lear (USA) for their input to the Global Cybersecurity Index (GCI) work and report.

The online questionnaire preparation, secondary data collection, data validation and report elaboration have been carried out with the support of Mohaamed Ahmed Yousef Aly, Ahmed Abd Allah Abd El- Latif, Tymoteusz Kurpeta, Benjamin Lim, Daniela Toma, Grace Rachael Acayo, and Lena Lattion.

If you have any comments, please contact the ITU Cybersecurity Team: cybersecurity@itu.int

ISBN

978-92-61-25061-4 (paper version)

978-92-61-25071-3 (electronic version)

978-92-61-25081-2 (EPUB version)

978-92-61-25091-1 (Mobi version)

Please consider the environment before printing this report.

© ITU 2017

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Foreword

The global community is increasingly embracing ICTs as key enabler for social and economic development. Governments across the world recognize that digital transformation has the power to further the prosperity and wellbeing of their citizens. In supporting this transformation, they also recognize that cybersecurity must be an integral and indivisible part of technological progress.

In 2016, nearly one percent of all emails sent were essentially malicious attacks, the highest rate in recent years. Ransomware attacks increasingly affected businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. Attackers are demanding more and more from victims, with the average ransom demand rising to over 1,000 USD in 2016, up from approximately 300 USD a year earlier. In May 2017, a massive cyberattack caused major disruptions to companies and hospitals in over 150 countries, prompting a call for greater cooperation around the world.

First launched in 2014, the goal of the Global Cybersecurity Index (GCI) is to help foster a global culture of cybersecurity and its integration at the core of ICTs. This second iteration of the GCI measures the commitment of ITU Member States towards cybersecurity in order to drive further efforts in the adoption and integration of cybersecurity on a global scale.

The GCI reaffirms ITU's commitment to build confidence and security in the use of ICTs. This report on the second iteration of the GCI continues to show the cybersecurity commitment of ITU Member States around the world, and I am pleased to note that the overall picture shows improvement and strengthening of the global cybersecurity agenda.

I wish to thank Member States for their contribution to this effort.

The collection of information for the GCI is an ongoing process, and I therefore invite all ITU Member States to continue sending and updating information on their cybersecurity efforts so that we can effectively share experiences, views and solutions in order to make the digital world a more secure and safe environment for all citizens.

Brahima Sanou

Director, Telecommunication Development Bureau

Executive Summary

The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.

The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation). For each of these pillars, questions were developed to assess commitment. Through consultation with a group of experts, these questions were weighted in order to arrive at an overall GCI score. The survey was administered through an online platform through which supporting evidence was also collected.

One-hundred and thirty-four Member States responded to the survey throughout 2016. Member States who did not respond were invited to validate responses determined from open-source research. As such, the GCI results reported herein cover all 193 ITU Member States.

The 2017 publication of the GCI continues to show the commitment to cybersecurity of countries around the world. The overall picture shows improvement and strengthening of all five elements of the cybersecurity agenda in various countries in all regions. However, there is space for further improvement in cooperation at all levels, capacity building and organizational measures. As well, the gap in the level of cybersecurity engagement between different regions is still present and visible. The level of development of the different pillars varies from country to country in the regions, and while commitment in Europe remains very high in the legal and technical fields in particular, the challenging situation in the Africa and Americas regions shows the need for continued engagement and support.

In addition to providing the GCI score, this report also provides a set of illustrative practices that give insight into the achievements of certain countries.

Table of Contents

Foreword iii

Executive Summary v

1 Introduction 1

2 GCI Scope and Framework 3
- 2.1 Background 3
- 2.2 Reference model 3
- 2.3 Conceptual framework 4

3 Methodology 9

4 Key Findings 13
- 4.1 Heat Map of National Cybersecurity Commitments 13
- 4.2 GCI Groups 13

5 Global Outlook 17
- 5.1 Noteworthy figures 17
- 5.2 Comparing GCI with other indices 19

6 Regional Outlook 25
- 6.1 Africa 26
- 6.2 Americas 28
- 6.3 Arab States 30
- 6.4 Asia and the Pacific 32
- 6.5 Commonwealth of Independent States 34
- 6.6 Europe 36

7 Illustrative practices by pillar 39
- 7.1 Legal 39
  - 7.1.1 Cybercrime legislation 39
  - 7.1.2 Cybersecurity regulation 39
  - 7.1.3 Cybersecurity training 39
- 7.2 Technical 40
  - 7.2.1 National CERT/CIRT/CSIRT 40
  - 7.2.2 Government CERT/CIRT/CSIRT 40
  - 7.2.3 Sectoral CERT/CIRT/CSIRT 40
  - 7.2.4 Cybersecurity standards implementation framework for organizations 41
  - 7.2.5 Child online protection 41
- 7.3 Organizational 41
  - 7.3.1 Strategy 41
  - 7.3.2 Public consultation 42
  - 7.3.3 Responsible agency 42
  - 7.3.4 Cybersecurity metrics 42
- 7.4 Capacity building 42
  - 7.4.1 Standardization bodies 42
  - 7.4.2 Good practice 42

7.4.3 Cybersecurity research and development programmes 43
7.4.4 Public awareness campaigns 43
7.4.5 Cybersecurity professional training courses 43
7.4.6 National education programmes and academic curricula 43
7.4.7 Incentive mechanisms 43
7.4.8 Home-grown cybersecurity industry 44
7.5 Cooperation 44
7.5.1 Bilateral agreements 44
7.5.2 Multilateral agreements 44
7.5.3 Participation in international fora 44
7.5.4 Public-private partnerships 45
7.5.5 Interagency partnerships 45

8 Conclusion 47

Abbreviations 49

Annex 1 – ITU Member States Global Cybersecurity Commitment Score By Region 51

Annex 2 – GCI 2017 Score 59

List of Tables, Figures and Boxes

Tables

Table 3.1: Numbers of responses received from all Members States regionally 10
Table 5.1: Top ten most committed countries, GCI (normalized score) 17
Table 6.1.1: Top three ranked countries in Africa 26
Table 6.2.1: Top three ranked countries in the Americas 28
Table 6.3.1: Top three ranked countries in the Arab States 30
Table 6.4.1: Top three ranked countries in Asia and the Pacific 32
Table 6.5.1: Top three ranked countries in Commonwealth of Independent States 34
Table 6.6.1: Top three ranked countries in Europe 36

Figures

Figure 2.3.1: GCI pillars and sub-pillars 5
Figure 2.3.2: GCA tree structure illustrating all pillars (simplified) 6
Figure 2.3.3: GCI tree structure illustrating Legal pillar 7
Figure 4.1.1: GCI Heat Map 13
Figure 4.2.1: GCI Tiers 14
Figure 5.1.1: Cybersecurity strategy and training commitments 18
Figure 5.1.2: Computer emergency response teams and metrics 18
Figure 5.1.3: Home-grown industry and international participation 19
Figure 5.2.1: Global comparison GCI and IDI 20
Figure 5.2.2: Comparison GCI and IDI in the Africa region 20
Figure 5.2.3: Comparison GCI and IDI in the Americas region 21
Figure 5.2.4: Comparison GCI and IDI in the Arab States 21
Figure 5.2.5: Comparison GCI and IDI in the Asia and the Pacific region 22
Figure 5.2.6: Comparison GCI and IDI in the Commonwealth of Independent States 22
Figure 5.2.7: Comparison GCI and IDI in the Europe region 23
Figure 6.1: Average pillar scores by region 25
Figure 6.1.1: Top three ranked countries in Africa and global ranked of all countries in Africa 26
Figure 6.1.2: Africa region scorecard 27
Figure 6.2.1: Top three ranked countries and an average score of all the Americas 28
Figure 6.2.2: Americas region scorecard 29
Figure 6.3.1: Top three ranked countries and an average score of the Arab States 30
Figure 6.3.2: Arab States scorecard 31
Figure 6.4.1: Top three ranked countries and an average score of all Asia and the Pacific 32
Figure 6.4.2: Asia and the Pacific Region Scorecard 33
Figure 6.5.1: Top three ranked countries and an average score of all CIS 34
Figure 6.5.2: CIS region scorecard 35
Figure 6.6.1: Top three ranked countries and an average score of all Europe 36
Figure 6.6.2: Europe region scorecard 37

1 Introduction

The information and communication technologies (ICT) networks, devices and services are increasingly critical for day-to-day life. In 2016, almost half the world used the Internet (3.5 billion users)[1] and according to one estimate, there will be over 12 billion machine-to-machine devices connected to the Internet by 2020[2]. Yet, just as in the real world, the cyber world is exposed to a variety of security threats that can cause immense damage.

Statistics on threats to computer networks are sobering and reflect a shift from the relatively innocuous spam of yesteryear to threats that are more malicious. A security company tracking incidents in 2016 found that malicious emails became a weapon of choice for a wide range of cyberattacks during the year used by everyone from state sponsored cyber espionage groups to mass-mailing ransomware gangs. One-in-131 emails sent were malicious, the highest rate in five years.

Ransomware continues to plague businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. In some cases, organizations can be overwhelmed by the sheer volume of ransomware-laden emails they receive. Attackers are demanding more and more from victims with the average ransom demand in 2016 rising to USD 1 077, up from USD 294 a year earlier[3]. The scale of cybercrime makes it critical for governments to have a robust cybersecurity ecosystem in place to reduce threats and enhance confidence in using electronic communications and services.

It is therefore clear that there is a direct cause-effect principle between the growth of ICTs and their illicit and malicious use. To counter this effect, cybersecurity is becoming more and more relevant in the minds of countries' decision makers, and cybersecurity related doctrines have been established in almost all countries in the world.

However, there is still an evident gap between countries in terms of awareness, understanding, knowledge and finally capacity to deploy the proper strategies, capabilities and programmes to ensure a safe and appropriate use of ICTs as enablers for economic development.

In this context, ITU, together with international partners from private-public and private sector as well as academia, has established the GCI with the key objective of building capacity at the national, regional and international level, through assessing the level of engagement of countries on cybersecurity, and, with the data gathered, producing a list of good practices that can be used by countries in need.

[1] www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
[2] www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html
[3] www.symantec.com

2 GCI Scope and Framework

2.1 Background

The GCI is included under Resolution 130 (Rev. Busan, 2014) on strengthening the role of ITU in building confidence and security in the use of ICT. Specifically, Member States are invited "to support ITU initiatives on cybersecurity, including the Global Cybersecurity Index (GCI), in order to promote government strategies and the sharing of information on efforts across industries and sectors".

A first iteration of the GCI was conducted in 2013-2014 in partnership with ABI Research[1], and the final results have been published[2].

Following feedback received from various communities, a second iteration of the GCI was planned and undertaken. This new version was formulated around an extended participation from Member States, experts and industry stakeholders as contributing partners (namely World Bank and Red Team Cyber as new GCI partners joining the Australia Strategic Policy Institute, FIRST, Indiana University, INTERPOL, ITU-Arab Regional Cybersecurity Centre in Oman, Korea Internet & Security Agency, NTRA Egypt, The Potomac Institute of Policy Studies, UNICRI, University of Technology Jamaica and UNODC) who all provided support with the provision of secondary data, response activation, statistical analysis, qualitative appreciation amongst other.

The data collected via GCI 2017 for ITU-D Study Group 2 Question 3 (SG2Q3) surveys have been analysed by the Rapporteur and co-Rapporteur for inclusion in the SG2Q3 final report. GCI partners have been active in providing expertise and secondary data as appropriate, while the UN office of ICT (New York) has also initiated collaborative work. ITU is also working in a multi-stakeholder collaboration led by the World Bank to elaborate a toolkit on "Best practice in Policy/Legal enabling Framework and Capacity Building in Combatting Cybercrime". ITU is providing support on the component on capacity building from a cybersecurity perspective based on GCI 2017 data.

An enhanced reference model was thereby devised. Throughout the steps of this new version, Member States were consulted using various vehicles including ITU-D Study Group 2 Question 3/2, where the overall project was submitted, discussed and validated.

2.2 Reference model

The GCI is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States cybersecurity commitment with regard to the five pillars identified by the High-Level Experts Group and endorsed by the GCA. These pillars form the five pillars of GCI.

The main objectives of the GCI are to measure:

- the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- the progress in cybersecurity commitment of all countries from a global perspective;
- the progress in cybersecurity commitment from a regional perspective;
- the cybersecurity commitment divide, i.e. the difference between countries in terms of their level of engagement in cybersecurity programmes and initiatives.

[1] https://www.abiresearch.com/
[2] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014.aspx

The objective of the GCI as an initiative is to help countries identify areas for improvement in the field of cybersecurity, as well as to motivate them to take action to improve their ranking, thus helping raise the overall level of commitment to cybersecurity worldwide.

Through the information collected, the GCI aims to illustrate the practices of other countries so that Member States can implement selected aspects suitable to their national environment, with the added benefits of helping harmonize practices and fostering, a global culture of cybersecurity.

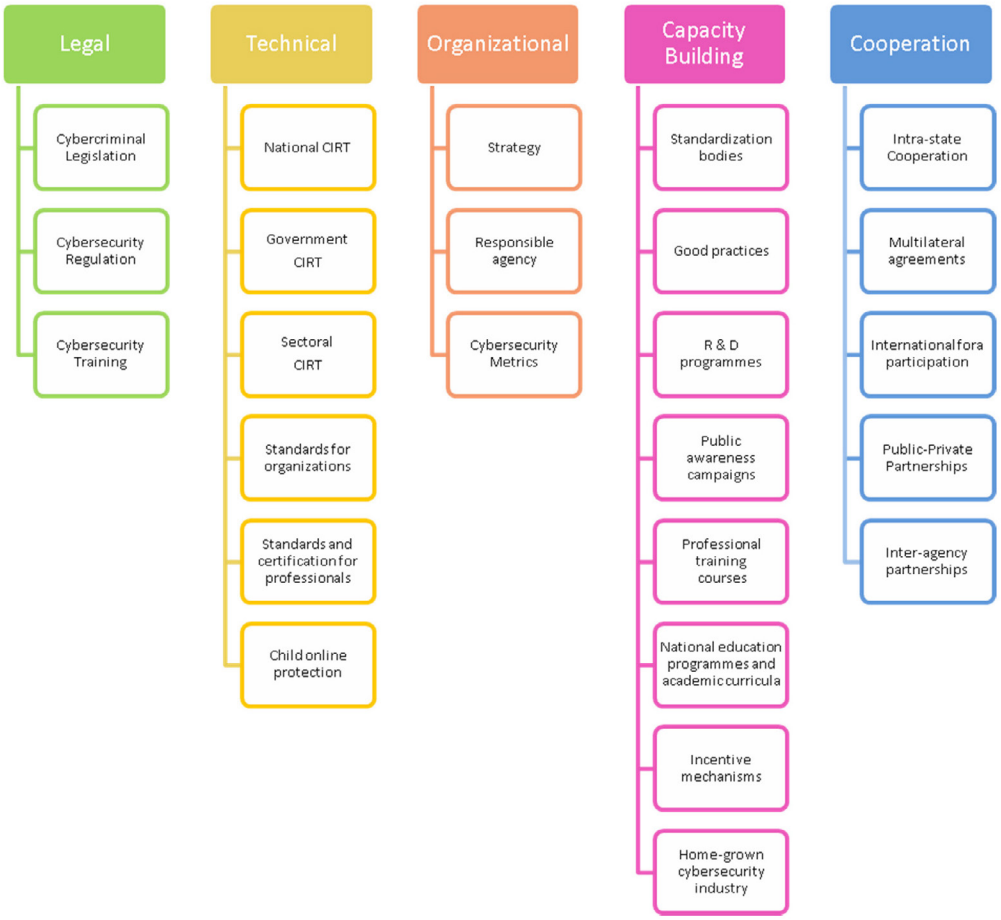
2.3 Conceptual framework

The five pillars of the GCI are briefly explained below:

1. **Legal:** Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.
2. **Technical:** Measured based on the existence of technical institutions and frameworks dealing with cybersecurity.
3. **Organizational:** Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.
4. **Capacity Building:** Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.
5. **Cooperation:** Measured based on the existence of partnerships, cooperative frameworks and information sharing networks.

Each pillar was then further divided in sub-pillars (Figure 2.3.1).

Figure 2.3.1: GCI pillars and sub-pillars



The questionnaire was elaborated on the basis of these sub-pillars[3]. The values for the 25 indicators were therefore constructed through 157 binary questions. This was done in order to achieve the required level of granularity and ensure accuracy and quality on the answers.

[3] http://www.itu.int/en/ITU-D/Cybersecurity/Documents/QuestionnaireGuide-E.pdf

Figure 2.3.2 below represents all the five pillars from GCA with their indicators.

Figure 2.3.2: GCA tree structure illustrating all pillars (simplified)

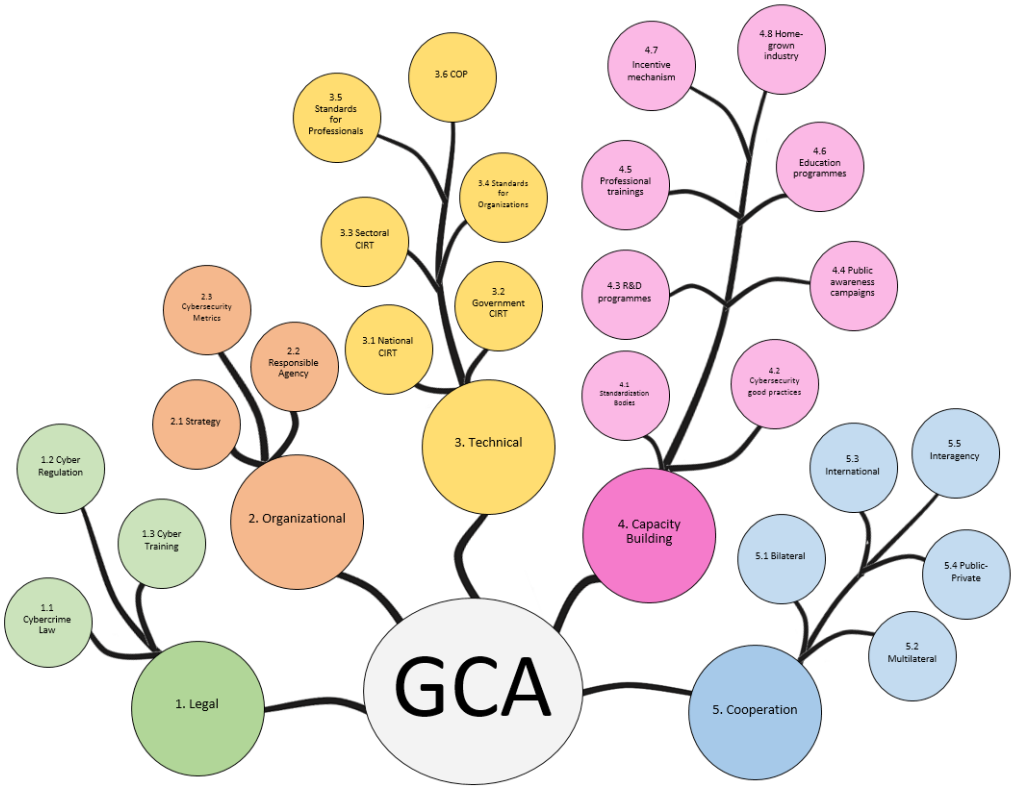
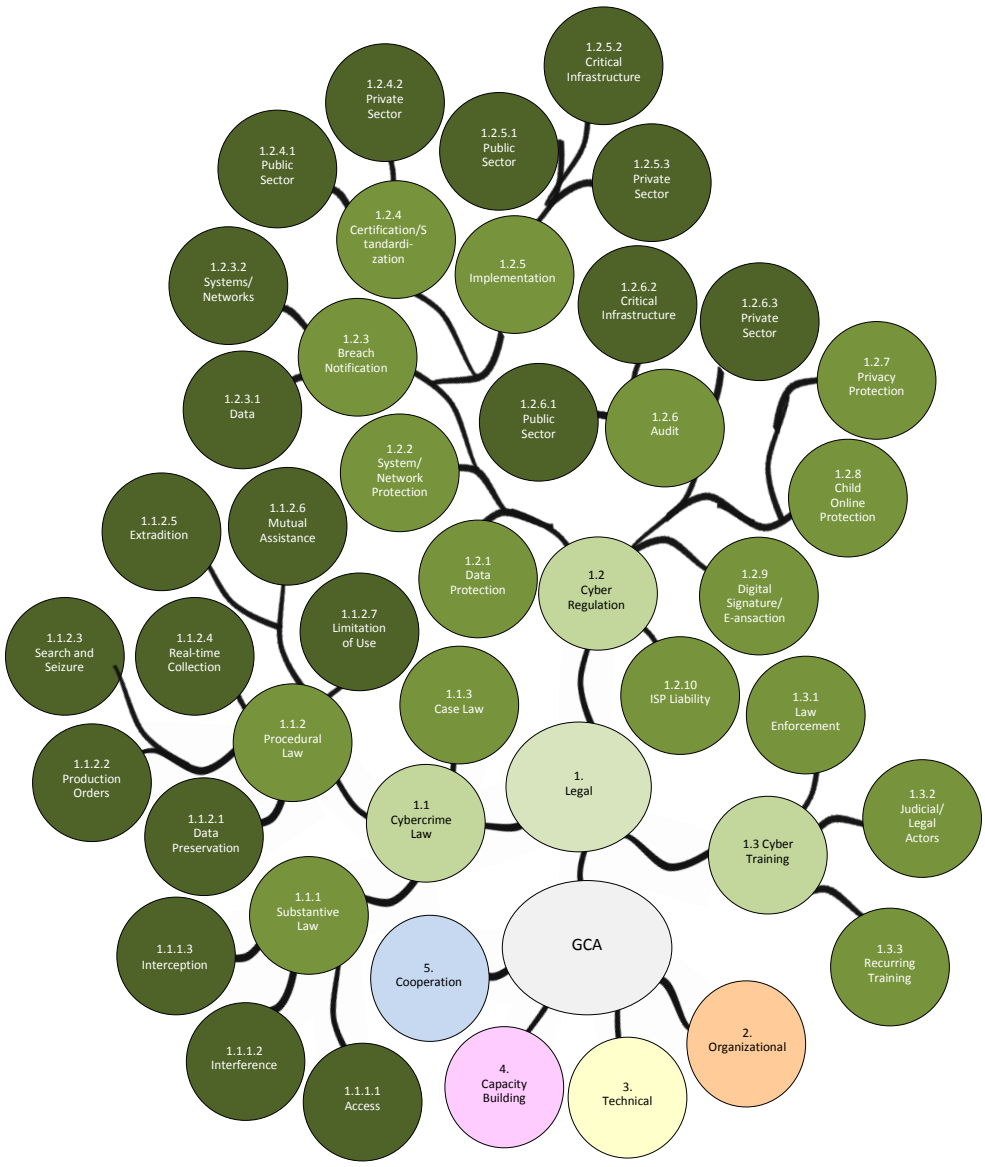


Figure 2.3.3 below illustrates the relationship between the GCA, the pillars, sub-pillars and questions (expanded only for the legal pillar due to space considerations).

Figure 2.3.3: GCI tree structure illustrating Legal pillar



3 Methodology

The GCI includes 25 indicators and 157 questions. The indicators used to calculate the GCI were selected on the basis of the following criteria:

- relevance to the five GCA pillars and in contributing towards the main GCI objectives and conceptual framework;
- data availability and quality;
- possibility of cross verification through secondary data.

The whole concept of a new iteration of the GCI is based on a cybersecurity development tree map and binary answer possibilities.

The tree map concept, which is illustrated in Figures 2.3.2 and 2.3.3, is an example of different possible paths that might be taken by countries in order to enhance their cybersecurity commitment.

Each of the five pillars are associated with a specific colour. The deeper the path taken, indicating a more developed level of commitment, the deeper the colour depicting it becomes.

The various levels of cybersecurity development among countries, as well as the different cybersecurity needs reflected by a country's overall ICT development status, were taken into consideration. The concept is based on the assumption that the more developed cybersecurity is, the more complex the solutions observed will be. Therefore, the further a country goes along the tree map by confirming the presence of pre-identified cyber solutions, the more complex and sophisticated the cybersecurity commitment is within that country, allowing it to obtain a higher score with the GCI.

The rationale behind using binary answer possibilities is the elimination of opinion-based evaluation and of any possible bias towards certain types of answers.

Moreover, the simple binary concept will allow quicker and more complex evaluation as it will not require lengthy answers from countries. This, in turn, is assumed to accelerate and streamline the process of providing answers and further evaluation. The idea is that the respondent will only confirm the presence or lack of certain pre-identified cybersecurity solutions. An online survey mechanism, which was used for gathering answers and uploading all relevant materials, enabled the extraction of good practices.

The key difference in methodology between GCI 2014 and GCI Version 2017 is the use of a binary system instead of a three-level system. The binary system evaluates the existence or absence of a specific activity, department or measure. Unlike GCI Version 2014, it does not take 'partial' measures into consideration. The facility for respondents to upload supporting documents and URLs is a way of providing more information to substantiate the binary response. Furthermore, a number of new questions have been added in each of the five pillars in order to refine the depth of research.

The GCI 2014 and GCI 2017 are not directly comparable due to a change in methodology. While the 2014 index used a simple average methodology, the 2017 index employs a weighting factor for each pillar.

The questionnaire, made available through an online survey from January to September 2016, was administered to the 193 ITU Member States (plus State of Palestine) in the regions of Africa, Americas, Arab States, Asia and the Pacific, the Commonwealth of Independent States, and Europe. 134 countries responded to the online survey while 59 countries did not provide primary data.

Table 3.1: Numbers of responses received from all Members States regionally

Region	Africa	Americas	Arab States	Asia and the Pacific	CIS	Europe	Global
Responses	29	23	16	25	7	34	134
Non-responses	15	12	5	13	5	9	59
Total of participants	44	35	21	38	12	43	193

The data collection process was implemented as follows:

1. A ***Letter of Invitation*** was sent by the ITU Secretariat to all Member States, informing them on the initiative and requesting the identification of a country level GCI focal point with whom ITU could liaise and who would be responsible for collecting all relevant data for completing the online GCI questionnaire. A guideline to the online questionnaire which provided explanations and examples for each question, was attached to the letter [1].
2. ***Primary data collection*** (for countries who responded to the questionnaire):
   - Verification of the responses received by the specific Member State to identify possible missing elements (no or missing responses, no or missing supporting documents, no or missing links, etc.).
     - For instance, if a Member State answered "No", ITU researched to prove that they do not have any documents in the ITU database or online.
     - If a Member State answered "Yes", ITU researched to verify that answers provided were correct and corresponded to the question.
   - The focal point identified by the concerned Member State was contacted and provided with indications on how to improve the accuracy of the responses. Where necessary ITU provided comments and guidance to improve the completed questionnaire.
   - After the necessary rounds of iterations, the pre-final questionnaire was sent back to the concerned Member State for final approval.
   - Once formal approval was received, the questionnaire was considered validated and used for the analysis, scoring and ranking.
3. ***Secondary data collection*** (for countries that did not respond to the questionnaire):
   - ITU elaborated an initial draft of the response to the questionnaire using publicly available data and online research.
   - The draft was then sent to the concerned Member State for review.
   - The reviewed response received, the focal point identified by the concerned Member State was contacted and provided with indications on how to improve the accuracy of the responses. Where necessary ITU provided comments and guidance to improve the completed questionnaire.
   - After the necessary rounds of iterations, the pre-final questionnaire was sent back to the concerned Member State for final approval.

[1] http://www.itu.int/en/ITU-D/Cybersecurity/Documents/QuestionnaireGuide-E.pdf

- Once formal approval was received, the questionnaire was considered validated and used for the analysis, scoring and ranking.

The GCI 2017 methodology encompassed the use of a panel of experts, identified according to their specific expertise on the subject, who acted in their personal capacity in order to provide an expert view on the weighting to be used for the scoring.

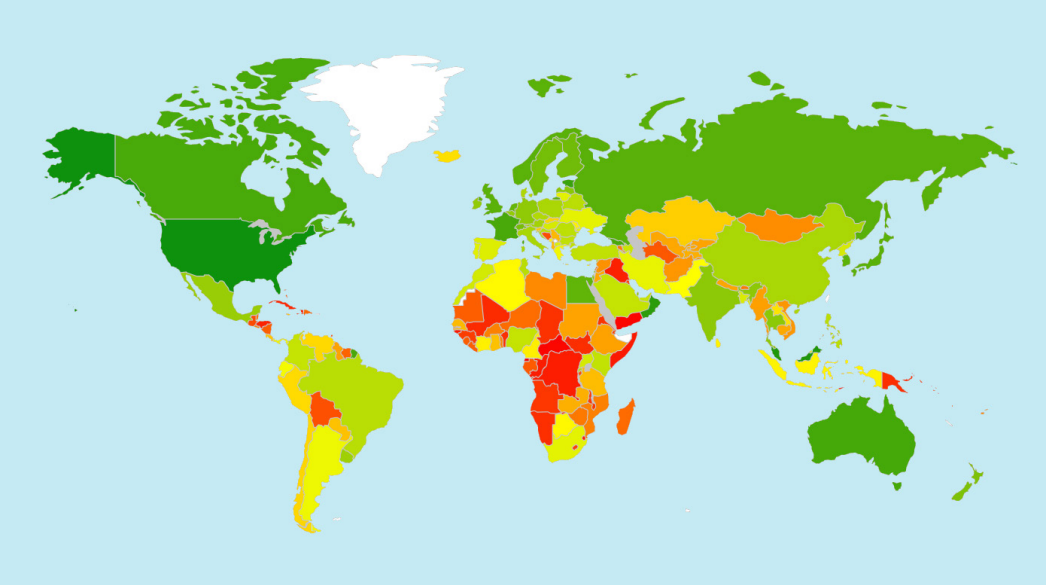
4 Key Findings

4.1 Heat Map of National Cybersecurity Commitments

Out of the 193 Member States, there is a huge range in cybersecurity commitments, as the heat map below illustrates.

Level of commitment: from Green (highest) to Red (lowest)

Figure 4.1.1: GCI Heat Map



4.2 GCI Groups

Member States were classified into three categories by their GCI score (Figure 4.2.1).

- *Initiating stage* refers to the 96 countries (i.e., GCI score less than the 50th percentile) that have started to make commitments in cybersecurity.
- *Maturing stage* refers to the 77 countries (i.e., GCI score between the 50th and 89th percentile) that have developed complex commitments, and engage in cybersecurity programmes and initiatives.
- *Leading stage* refers to the 21 countries (i.e., GCI score in the 90th percentile) that demonstrate high commitment in all five pillars of the index.

Figure 4.2.1: GCI Tiers

INITIATING		
Afghanistan	Guatemala	Palau
Andorra	Guinea	State of Palestine
Angola	Guinea-Bissau	Papua New Guinea
Antigua and Barbuda	Guyana	Saint Kitts and Nevis
Armenia	Haiti	Saint Lucia
Bahamas	Honduras	Saint Vincent & the Grenadines
Barbados	Iraq	Samoa
Belize	Jordan	San Marino
Benin	Kiribati	Sao Tome and Principe
Bhutan	Kuwait	Seychelles
Bolivia (Plurinational State of)	Kyrgyzstan	Sierra Leone
Bosnia & Herzegovina	Lebanon	Solomon Islands
Burkina Faso	Lesotho	Somalia
Burundi	Liberia	South Sudan
Cambodia	Libya	Sudan
Cape Verde	Liechtenstein	Suriname
Central African Republic.	Madagascar	Swaziland
Chad	Malawi	Syrian Arab Republic
Comoros	Maldives	Tajikistan
Congo	Mali	Timor-Leste
Cuba	Marshall Islands	Togo
Democratic Republic of the Congo	Mauritania	Tonga
Djibouti	Micronesia	Trinidad and Tobago
Dominica	Monaco	Turkmenistan
Dominican Republic	Mongolia	Tuvalu
El Salvador	Mozambique	Uzbekistan
Equatorial Guinea	Myanmar	Vanuatu
Eritrea	Namibia	Vatican
Ethiopia	Nauru	Viet Nam
Fiji	Nepal (Republic of)	Yemen
Gabon	Nicaragua	Zambia
Gambia	Niger	Zimbabwe
Grenada		

MATURING		
Albania	Ghana	Peru
Algeria	Greece	Philippines
Argentina	Hungary	Poland
Austria	Iceland	Portugal
Azerbaijan	India	Qatar
Bahrain	Indonesia	Romania
Bangladesh	Iran (Islamic Republic of)	Rwanda
Belarus	Ireland	Saudi Arabia
Belgium	Israel	Senegal
Botswana	Italy	Serbia
Brazil	Jamaica	Slovakia
Brunei Darussalam	Kazakhstan	Slovenia
Bulgaria	Kenya	South Africa
Cameroon	Laos	Spain
Chile	Latvia	Sri Lanka
China	Lithuania	Tanzania
Colombia	Luxembourg	Thailand
Costa Rica	Malta	The Former Yugoslav Rep. of Macedonia
Côte d'Ivoire	Mexico	Tunisia
Croatia	Moldova	Turkey
Cyprus	Montenegro	Uganda
Czech Republic	Morocco	Ukraine
Dem. People's Rep. of Korea	Nigeria	United Arab Emirates
Denmark	Pakistan	Uruguay
Ecuador	Panama	Venezuela
Germany	Paraguay	

LEADING		
Australia	Japan	Oman
Canada	Korea	Russian Federation
Egypt	Malaysia	Singapore
Estonia	Mauritius	Sweden
Finland	Netherlands	Switzerland
France	New Zealand	United Kingdom
Georgia	Norway	United States

5 Global Outlook

All of the six ITU regions are represented in the top ten commitment level in the GCI. There are three from Asia and the Pacific, two each from Europe and the Americas, and one from Africa, the Arab States, and the Commonwealth of Independent States.

This suggests that being highly committed is not strictly tied to geographic location.

Table 5.1: Top ten most committed countries, GCI (normalized score)

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

As the GCI shows, there is a wide gulf in cyber preparedness around the globe. This gap exists between and within regions.

Further, cybersecurity related commitments are often unequally distributed with countries performing well in some pillars and less so in others. Cybersecurity is an ecosystem where laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective.

Additionally, cybersecurity is not just a concern of the government but also needs commitment from the private sector and consumers. Thus, it is important to develop a cybersecurity culture where citizens are aware of the trade-off between risks and monitoring when using electronic networks.

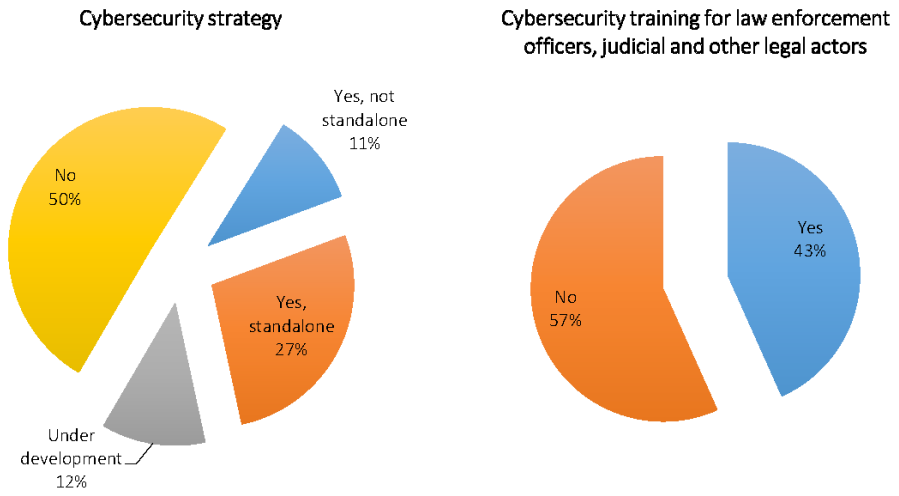
5.1 Noteworthy figures

The GCI consists of 25 different indicators. Some relate to precise commitments that help to concretize the status of specific cybersecurity activities throughout the world.

One of the strongest commitments is to outline a cybersecurity strategy describing how the country will prepare and respond to attacks against its digital networks. Only 38% countries have a published cybersecurity strategy and only 11% have a dedicated standalone strategy (Figure 5.1.1, left); another 12% have a cybersecurity strategy under development.

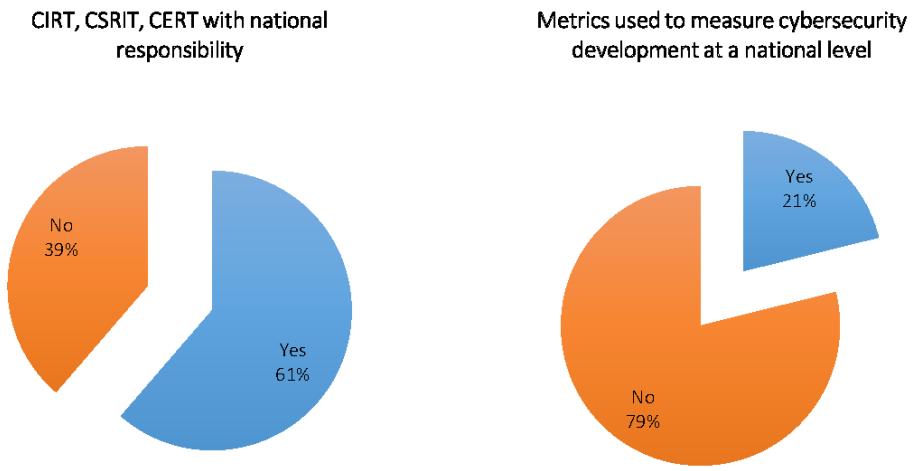
More effort is needed in this critical area, particularly since it conveys that the government considers digital risks high priority. In the area of training, efforts need to be enhanced particularly for those who are most likely going to legally handle cybersecurity crimes given that less than half the Member States (43%) have capacity-building programmes for law enforcement and the judicial system (Figure 5.1.1, right).

Figure 5.1.1: Cybersecurity strategy and training commitments



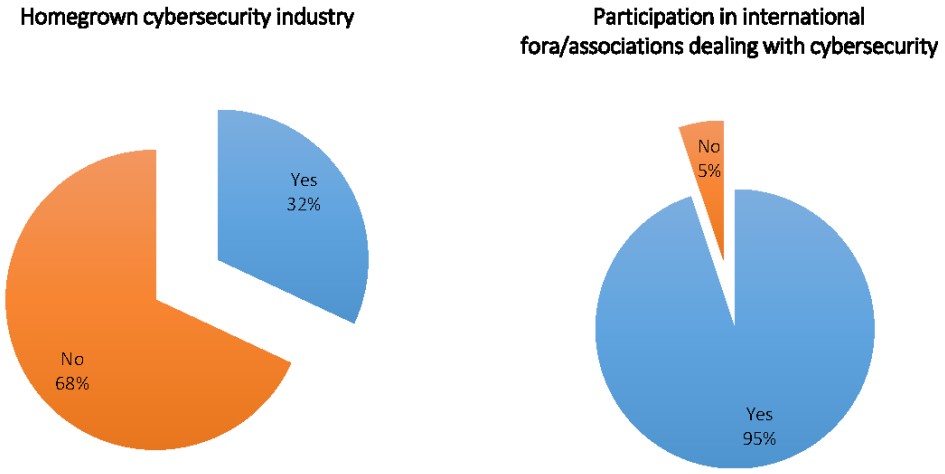
Despite half of the Member States not having a cybersecurity strategy, 61% do have an emergency response team (i.e., CIRT, CSRIT, and CERT) with national responsibility (Figure 5.1.2, left). However, just over a fifth (21%) publish metrics on cybersecurity incidents (Figure 5.1.2, right). This makes it difficult in most countries to objectively assess incidents based on the evidence and determine if protection measures are working.

Figure 5.1.2: Computer emergency response teams and metrics



Just less than a third of countries (32%) replied affirmatively to the existence of a homegrown cybersecurity industry (Figure 5.1.3, left). More efforts need to be devoted to this area as a local industry will have knowledge of national circumstances and make the security ecosystem more sustainable. The potential for global cooperation is heightened by participation in international cybersecurity events. This is almost universal with 95% of countries replying affirmatively (Figure 5.1.3, right).

Figure 5.1.3: Home-grown industry and international participation



5.2 Comparing GCI with other indices

A qualitative comparison has been performed to raise awareness on the importance of investing on cybersecurity, as an integral component of any national ICT for development strategy.

This paragraph is not intended to provide thorough, exhaustive statistical analysis, but rather an indication on how cybersecurity can relate to existing national processes, in order to emphasize the importance of investing and being committed.

Comparing GCI scores to notable ICT for Development Indices does not reveal an especially close relationship as experience shows that countries which score high in term of ICT for Development do not necessarily invest in cybersecurity with the same level of commitment, and vice versa.

For example, comparing the GCI with the ITU ICT for Development Index (IDI), shows that some countries are performing much better in the GCI than their level of ICT development would suggest.

The following figures show the relation between the GCI and IDI with each graph identifying the top three countries for each region.

Figure 5.2.1: Global comparison GCI and IDI

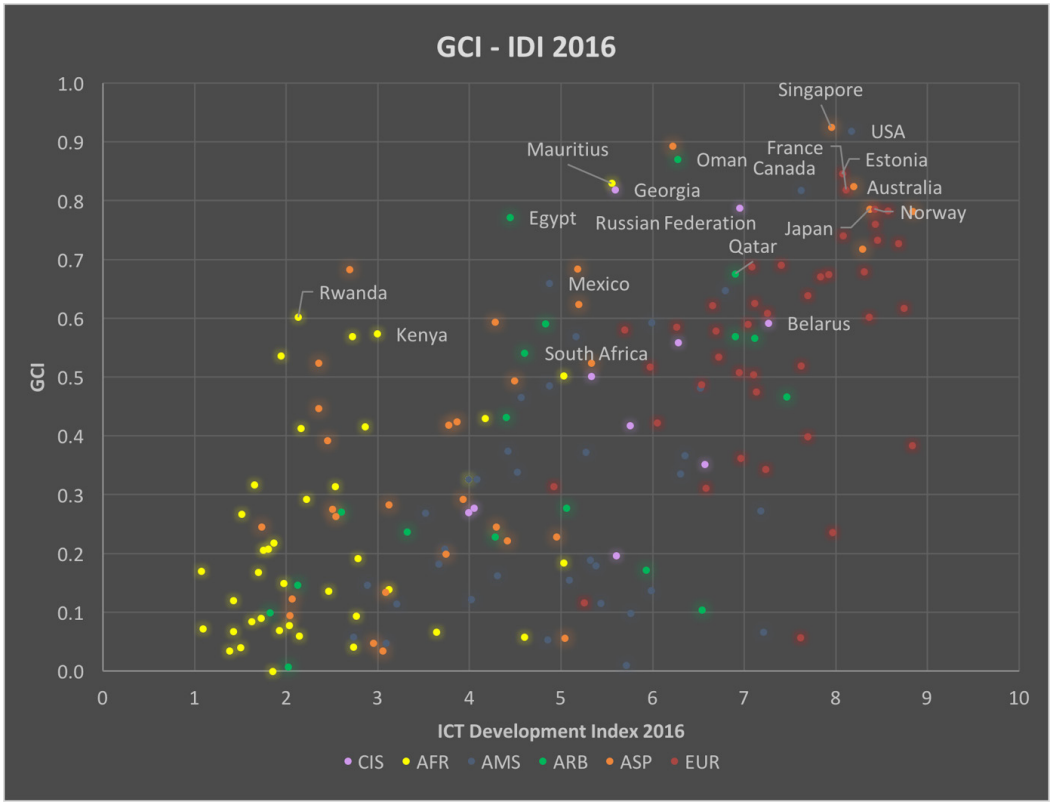


Figure 5.2.2: Comparison GCI and IDI in the Africa region

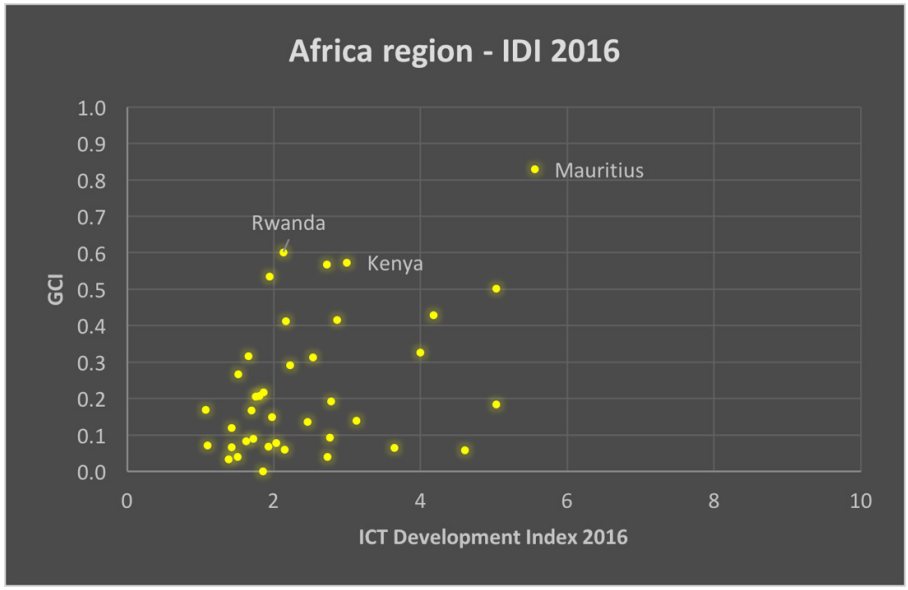


Figure 5.2.3: Comparison GCI and IDI in the Americas region

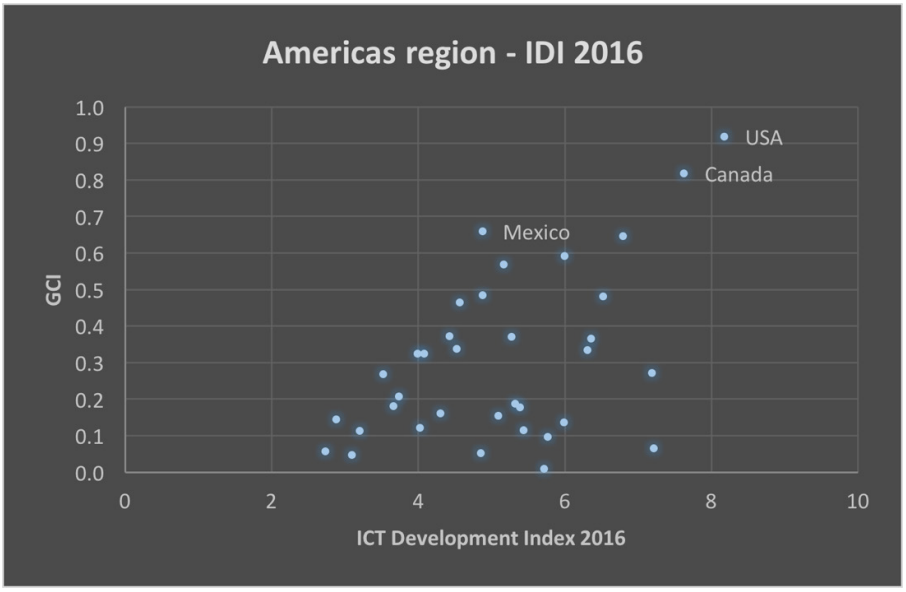


Figure 5.2.4: Comparison GCI and IDI in the Arab States

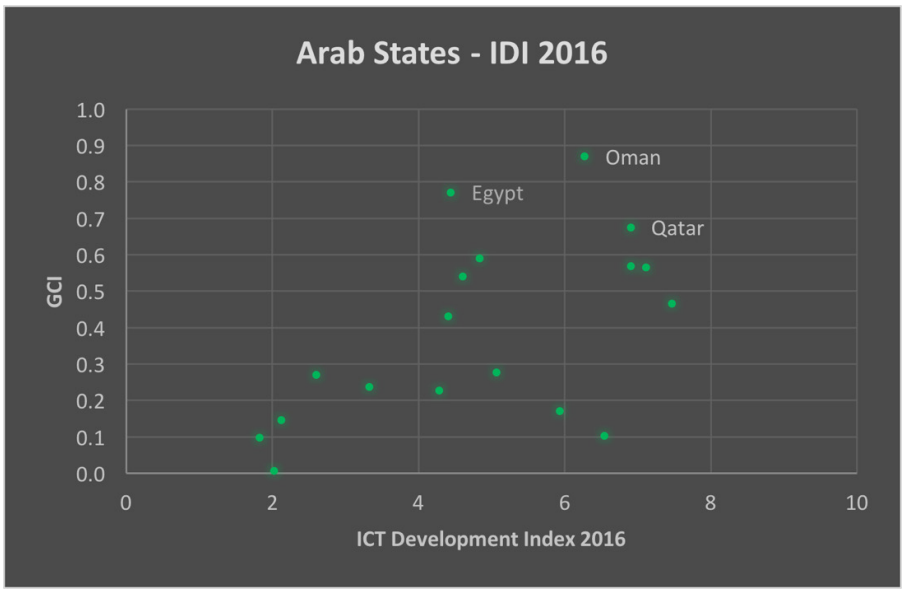


Figure 5.2.5: Comparison GCI and IDI in the Asia and the Pacific region

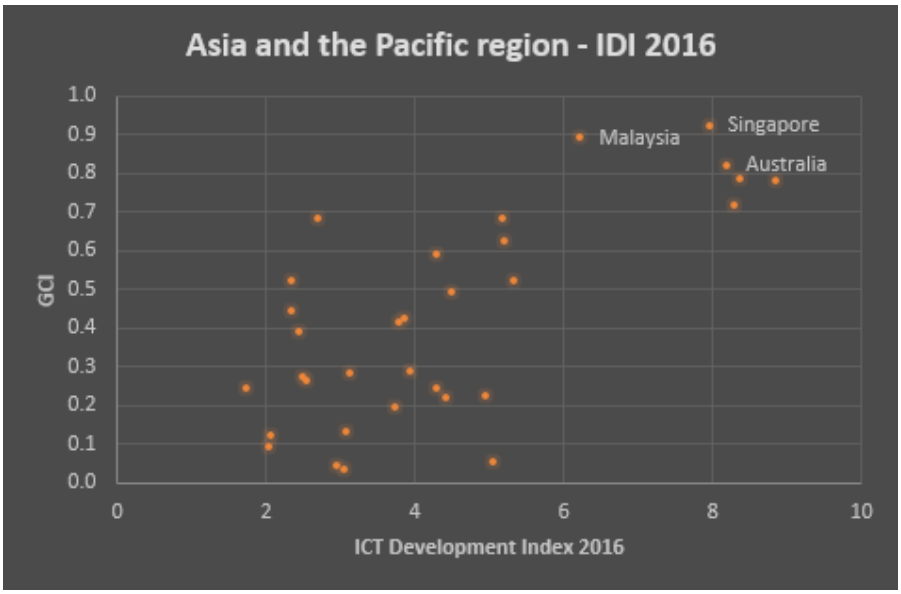


Figure 5.2.6: Comparison GCI and IDI in the Commonwealth of Independent States

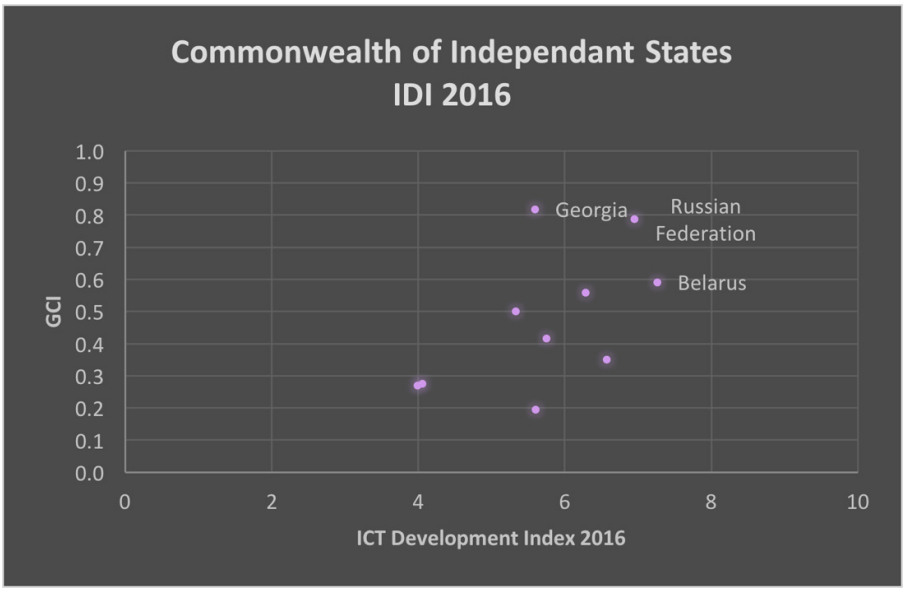
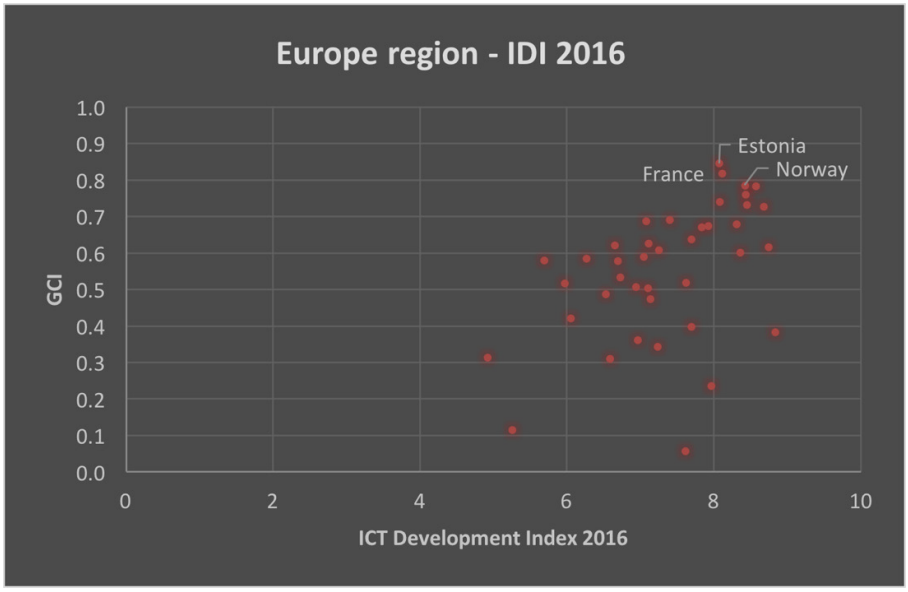


Figure 5.2.7: Comparison GCI and IDI in the Europe region



6 Regional Outlook

During the active data collection phase of the GCI 2017 exercise, there was a varied response from countries in the ITU regions:

- Out of the 44 Member States in the Africa region, 29 responded to the survey.
- Out of 35 Member States in the Americas region, 23 responded to the survey
- Out of 21 Member States in the Arab States region, 17 including the State of Palestine responded to the survey.
- Out of 38 Member States in the Asia and the Pacific region, 25 responded to the survey
- Out of the 12 Member States in the Commonwealth of Independent States region, 7 responded to the survey
- Out of 43 Member States in the Europe region, 34 responded to the survey.

Figure 6.1 illustrates the average GCI score for all countries in a particular region for the respective pillar. Scores that fall below the 33rd percentile have a red background, scores that are between the 33rd to 65th percentiles have a yellow background and scores that lie above the 65th percentile have a green background. There is scope for improvement since most regions have an average score for the different pillars (i.e., lying between 33rd and 65th percentiles).

The exception is Europe, where average scores are high across all pillars. The Africa region averages low scores for the organizational pillar while the Commonwealth of Independent States region averages a high score for the legal pillar.

The following sub-sections show the findings for each individual ITU region, highlighting the results and findings for the three top-scoring countries in each region. As well, a "regional scorecard" summarizes the countries' level of commitment to every pillar and sub-pillars (green for high, yellow for medium, and red for low).

Figure 6.1: Average pillar scores by region

Region	Legal	Technical	Organizational	Capacity Building	Cooperation
AFR	0.29	0.18	0.16	0.17	0.25
AMS	0.40	0.30	0.24	0.28	0.26
ARB	0.44	0.33	0.27	0.34	0.29
ASP	0.43	0.38	0.31	0.34	0.39
CIS	0.58	0.42	0.37	0.38	0.40
EUR	0.61	0.60	0.45	0.49	0.46

6.1 Africa

Table 6.1.1: Top three ranked countries in Africa

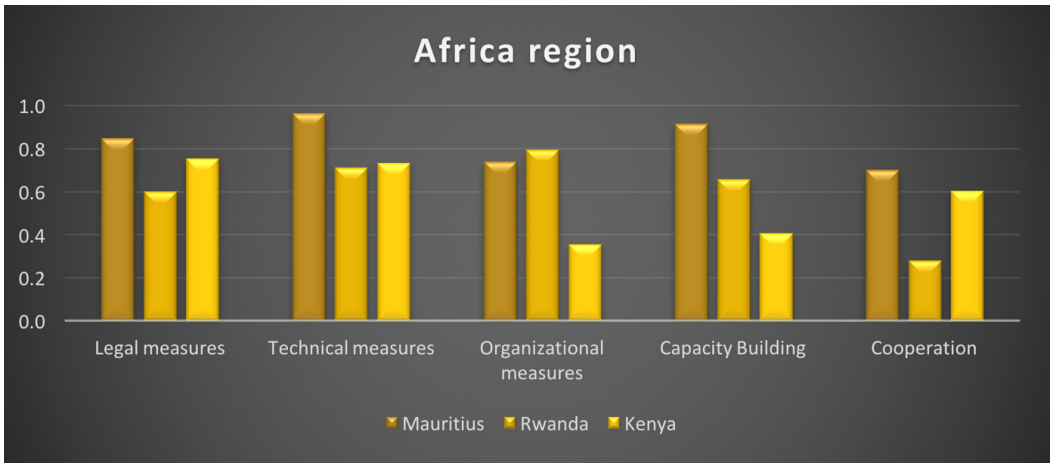
Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Mauritius	0.83	0.85	0.96	0.74	0.91	0.7
Rwanda	0.6	0.6	0.71	0.79	0.66	0.28
Kenya	0.57	0.75	0.73	0.36	0.41	0.6

Mauritius is the top ranked country in the Africa region. It scores particularly high in the legal and the technical areas. The Botnet Tracking and Detection project allows Computer Emergency Response Team of Mauritius (CERT-MU) to proactively take measures to curtail threats on different networks within the country. Capacity building is another area where Mauritius does well. The government IT Security Unit has conducted 180 awareness sessions for some 2 000 civil servants in 32 government ministries and departments.

Rwanda, ranked second in Africa, scores high in the organizational pillar and has a standalone cybersecurity policy addressing both the public and private sector[1]. It is also committed to develop a stronger cybersecurity industry to ensure a resilient cyber space.

Kenya, ranked third in the region, provides a good example of cooperation through its National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC)[2]. The CIRT coordinates at national, regional and global levels with a range of actors. Nationally this includes ISPs and the financial and educational sectors; regionally it works with other CIRTs through the East African Communications Organization; and internationally it liaises with ITU, FIRST, and bi-laterally with the United States and Japan CIRTs among others.

Figure 6.1.1: Top three ranked countries in Africa and global ranked of all countries in Africa



[1] http://www.myict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/Rwanda_Cyber_Security_Policy_01.pdf

[2] http://www.ke-cirt.go.ke/index.php/members/

Figure 6.1.2: Africa region scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURES**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURES**	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	**COOPERATION**	**GCI**
Angola	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Benin	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Botswana	🟢	🟢	🟡	🟢	🔴	🔴	🔴	🟢	🔴	🟢	🔴	🟢	🟢	🔴	🟡	🟢	🔴	🔴	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🟡
Burkina Faso	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Burundi	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Cameroon	🟡	🟡	🟢	🟢	🟡	🟢	🔴	🟢	🟡	🔴	🟡	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Cape Verde	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Central African Republic	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Chad	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Congo	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Cote d'Ivoire	🟡	🟢	🟢	🟢	🔴	🟢	🔴	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🟢	🟡	🔴	🔴	🟡	🟡	🔴	🟢	🔴	🔴	🔴	🟡
Democratic Republic of the Congo	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Equatorial Guinea	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Eritrea	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Ethiopia	🟡	🔴	🔴	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🟢	🟡	🔴	🟡	🟡	🟢	🟡	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Gabon	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Gambia	🟢	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Ghana	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟡	🟢	🟡	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Guinea	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Guinea-Bissau	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Kenya	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🔴	🟡	🟡	🟡	🟡	🔴	🟡	🟢	🟡	🟡	🟢	🔴	🟡	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Lesotho	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🔴	🟡	🔴
Liberia	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🟡	🔴	🟡	🔴
Madagascar	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🟡	🔴
Malawi	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🔴
Mali	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Mauritius	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Mozambique	🟡	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Namibia	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Niger	🟡	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟢	🔴
Nigeria	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟡	🟢	🟢	🟡	🟡	🔴	🟡	🔴	🔴	🟢	🟡	🟢	🟢	🟢
Rwanda	🟢	🟢	🔴	🟢	🟡	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🟢	🟡	🟢	🔴	🟢	🔴	🔴	🟢	🟡	🔴	🟡	🟢
Sao Tome and Principe	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Senegal	🟡	🟢	🟡	🟡	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟢	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🔴	🔴	🟢	🟡
Seychelles	🟢	🟡	🔴	🟡	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Sierra Leone	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🟡	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
South Africa	🟢	🟡	🟡	🟢	🟢	🟢	🔴	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🟡	🟡	🔴	🟢	🟡	🔴	🔴	🟢	🟡	🔴	🟡	🟡
South Sudan	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Swaziland	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Tanzania	🟢	🟡	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟢	🔴	🟡	🔴	🟢	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Togo	🔴	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Uganda	🟢	🟢	🔴	🟢	🟡	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🔴	🔴	🔴	🟢	🟢	🟡	🟢	🟢	🟡	🟡	🟢	🟢	🟡	🟢	🔴	🔴	🟢	🟢	🟡
Zambia	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🟢	🟡	🟡	🔴	🟡	🔴	🟢	🟢	🔴	🔴	🟡	🟡
Zimbabwe	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴

6.2 Americas

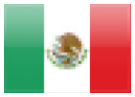
Table 6.2.1: Top three ranked countries in the Americas

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
United States	0.91	1	0.96	0.92	1	0.73
Canada	0.81	0.94	0.93	0.71	0.82	0.70
Mexico	0.66	0.91	0.89	0.48	0.68	0.34

The top three ranked countries in the Americas region are the members of the North American Free Trade Association (NAFTA).

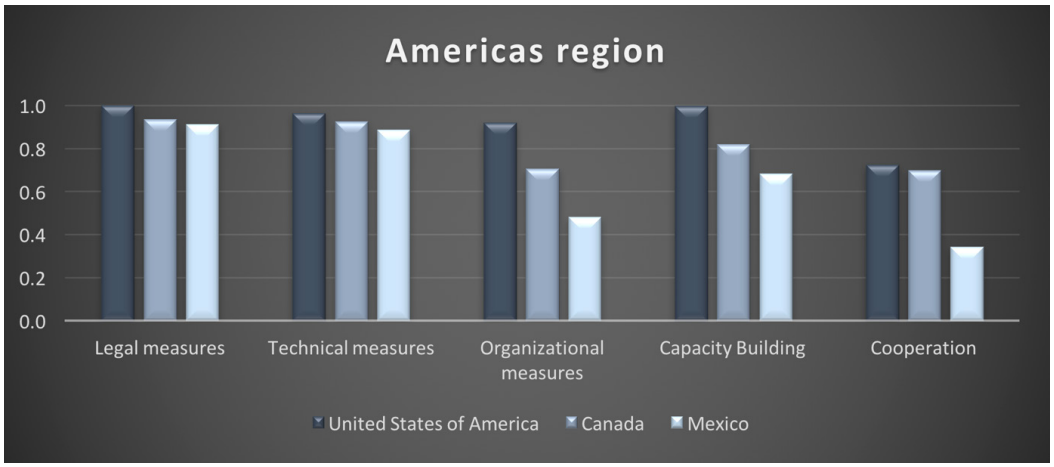
The United States of America has the highest scores for the legal and capacity building pillars. One notable aspect of both capacity building and cooperation in the country is the initiatives to coordinate cybersecurity among all states. To that end, the National Governor's Association established the Resource Center for State Cybersecurity, which offers best practices, tools and guidelines [3].

Canada ranks second in the region with its highest score in the legal pillar. The country's Personal Information Protection and Electronic Documents Act (PIPEDA) features several sections relating to cybersecurity[4]. It requires organizations to notify privacy authorities in the event of privacy breaches that could cause significant damage with penalties for those who fail to report them.



Mexico is third and some 16 points behind Canada, illustrating the cybersecurity divide in the region. Like the other top ranked countries in the region, it scores best in the legal pillar with a full suite of cyber legislation covering criminality, data protection, data privacy and electronic transactions.

Figure 6.2.1: Top three ranked countries and an average score of all the Americas



[3] https://www.nga.org/cms/statecyber
[4] http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Figure 6.2.2: Americas region scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURES**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURES**	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	**COOPERATION**	GCI
Antigua and Barbuda	Y	Y	R	Y	R	R	R	R	R	R	R	R	Y	R	Y	Y	R	R	Y	R	R	Y	R	Y	R	R	G	R	R	R	R	R
Argentina	G	Y	G	Y	G	G	G	R	R	R	Y	R	G	R	Y	Y	G	G	Y	Y	R	R	R	Y	R	R	G	R	G	Y	Y	Y
Bahamas	G	R	R	Y	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	G	R	R	R	R	R
Barbados	Y	R	G	Y	Y	R	R	R	R	G	R	R	Y	R	R	R	R	R	G	Y	R	R	R	R	R	R	G	R	R	R	R	R
Belize	R	Y	R	R	R	R	R	Y	Y	R	R	R	G	R	Y	R	R	R	Y	R	R	R	R	R	R	R	G	R	R	R	R	R
Bolivia	R	R	R	R	R	R	R	R	R	Y	R	R	Y	R	R	R	R	R	Y	R	R	R	R	R	R	R	G	R	R	R	R	R
Brazil	G	G	R	Y	G	G	G	Y	Y	G	G	Y	G	Y	Y	Y	G	G	G	Y	Y	R	R	Y	R	R	G	Y	G	Y	Y	Y
Canada	G	G	G	G	G	G	G	G	G	G	G	Y	G	G	G	Y	G	G	G	Y	Y	Y	G	G	Y	R	G	G	G	G	G	G
Chile	G	Y	R	Y	G	G	G	G	R	G	G	R	R	R	R	Y	G	G	G	Y	R	R	R	Y	R	R	G	Y	R	Y	Y	Y
Colombia	G	G	R	Y	G	G	R	G	G	R	G	R	R	Y	R	G	G	Y	G	G	R	Y	G	G	G	G	G	R	R	G	Y	Y
Costa Rica	G	Y	R	Y	Y	G	R	R	R	G	Y	R	Y	R	R	G	R	Y	Y	Y	Y	R	R	R	R	R	G	R	R	Y	Y	Y
Cuba	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	Y	R	R	R	R	R	R	R	R	R	R	G	R	R	R	R	R
Dominica	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
Dominican Republic	Y	Y	G	Y	R	R	R	R	R	R	R	R	Y	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
Ecuador	R	G	G	Y	G	R	G	G	Y	R	Y	R	G	R	Y	Y	G	Y	G	G	G	R	R	G	R	R	G	R	R	R	Y	Y
El Salvador	Y	Y	G	Y	R	R	R	R	R	R	R	R	Y	R	R	Y	R	R	R	G	R	R	R	R	R	R	G	R	R	R	R	R
Grenada	Y	Y	R	Y	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	G	R	R	R	R	R
Guatemala	R	R	R	R	Y	G	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	G	R	R	R	R	R
Guyana	Y	Y	G	Y	R	R	R	R	R	R	R	R	G	R	Y	R	R	R	R	G	R	Y	R	R	R	R	G	R	R	R	R	R
Haiti	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	G	R	R	R	R	R
Honduras	R	R	R	R	R	R	R	R	R	Y	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	G	R	R	R	R	R
Jamaica	G	R	R	R	R	G	R	R	R	R	R	G	Y	R	Y	Y	R	R	Y	G	G	R	R	Y	R	R	G	Y	R	Y	Y	Y
Mexico	G	G	G	G	G	G	G	Y	G	G	G	R	G	Y	Y	R	G	Y	G	G	G	Y	R	G	R	R	G	R	G	Y	G	G
Nicaragua	R	R	R	R	R	R	R	R	R	R	R	R	Y	R	R	R	R	R	R	Y	Y	R	R	R	R	R	G	R	G	Y	R	R
Panama	Y	Y	R	Y	R	G	R	G	R	R	Y	R	G	R	Y	Y	G	G	G	G	R	Y	R	Y	R	R	G	R	G	G	Y	Y
Paraguay	G	Y	R	Y	R	G	R	R	R	G	R	Y	Y	R	Y	R	G	G	G	R	R	R	R	R	R	R	G	R	R	R	Y	Y
Peru	Y	Y	R	Y	G	G	R	G	R	R	Y	R	G	R	Y	Y	G	R	R	Y	R	G	R	Y	R	R	G	R	R	R	Y	Y
Saint Kitts and Nevis	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	G	R	R	R	R	R
Saint Lucia	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	G	R	R	R	R	R
Saint Vincent and the Grenadines	G	Y	R	Y	R	R	R	R	R	R	R	R	R	R	R	R	R	R	G	Y	R	R	R	R	R	R	G	R	R	R	R	R
Suriname	R	R	R	R	R	R	R	R	R	R	R	R	G	R	Y	R	R	R	R	R	R	R	R	R	Y	R	G	R	R	R	R	R
Trinidad and Tobago	R	R	R	R	R	R	R	R	R	Y	R	Y	R	R	R	R	R	R	G	R	R	R	R	R	R	R	G	R	R	R	R	R
United States of America	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	Y	G	G	G	G
Uruguay	R	G	G	Y	G	G	G	Y	R	G	G	Y	G	R	Y	G	G	G	Y	Y	Y	Y	G	G	Y	R	G	G	G	G	G	G
Venezuela	G	Y	R	Y	G	G	G	R	R	Y	Y	R	Y	Y	Y	R	G	Y	Y	Y	R	R	R	R	R	R	G	R	R	R	Y	Y

6.3 Arab States

Table 6.3.1: Top three ranked countries in the Arab States

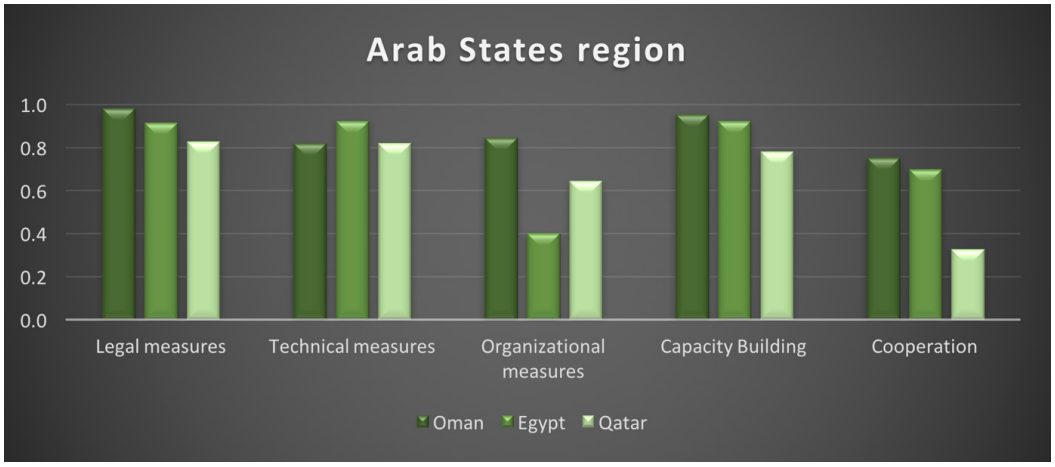
Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Egypt	0.77	0.92	0.92	0.4	0.92	0.7
Qatar	0.67	0.83	0.82	0.65	0.78	0.33

Sultanate of Oman is the top ranked in the Arab States with the highest scores in the legal and capacity building pillars. Oman has a robust organizational structure, including a high-level cybersecurity strategy and master plan and comprehensive roadmap.

Egypt ranks second with a full range of cooperation initiatives. It is a member of the UN Government Group of Experts (GGE) on cybersecurity[5], has chaired the ITU Working Group for Child Online Protection[6], was a founding member of AfricaCERT[7], and has a number of bi-lateral and multilateral agreements on cybersecurity cooperation.

Qatar ranks third and has been building a cybersecurity culture through campaigns such as Safer Internet Day and has spread warnings about online threats, such as fraud and Internet scams, via print and social media. The Qatar Cyber Crimes Investigation Center and Information Security Center support efforts to safeguard the public and crack down on those who use technology to carry out criminal activities.

Figure 6.3.1: Top three ranked countries and an average score of the Arab States



[5] https://www.un.org/disarmament/topics/informationsecurity/
[6] http://www.itu.int/en/council/cwg-cop/Pages/default.aspx
[7] https://www.africacert.org/home/

Figure 6.3.2: Arab States scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURES**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURES**	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	**COOPERATION**	**GCI**
Algeria	🟢	🟢	🟢	🟢	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟢	🔴	🟡	🔴	🟢	🟡	🟢	🟡	🔴	🔴	🔴	🟡	🟡	🔴	🟢	🔴	🔴	🟡	🟡
Bahrain	🟢	🟡	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🟡	🔴	🟡	🟡	🟡	🔴	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟢	🟡	🟡
Comoros	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Djibouti	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🔴
Egypt	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Iraq	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴
Jordan	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟡	🟢	🟡	🟡	🟢	🟡	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Kuwait	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴
Lebanon	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🔴
Libya	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟢	🟢	🔴	🟢	🟡	🔴	🔴	🟢	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Mauritania	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Morocco	🟢	🟢	🟢	🟢	🔴	🔴	🔴	🟢	🟢	🔴	🟢	🔴	🟢	🔴	🟡	🟡	🟢	🟡	🟢	🟡	🟡	🔴	🔴	🟡	🟡	🟢	🟢	🟢	🔴	🟡	🟡
Oman	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢
Qatar	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🔴	🟢	🟢	🔴	🔴	🟡	🟢
Saudi Arabia	🟡	🟡	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟢	🟢	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟡
Somalia	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
State of Palestine	🟢	🟡	🔴	🟡	🔴	🟢	🔴	🟡	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Sudan	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🟡	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Syrian Arab Republic	🟡	🟡	🟢	🟡	🔴	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Tunisia	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🟡	🔴	🟡	🟢	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🔴	🔴	🟡	🔴	🟢	🟢
United Arab Emirates	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🔴	🟡	🟡	🟢	🟢	🔴	🔴	🟡	🟡
Yemen	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴

6.4 Asia and the Pacific

Table 6.4.1: Top three ranked countries in Asia and the Pacific

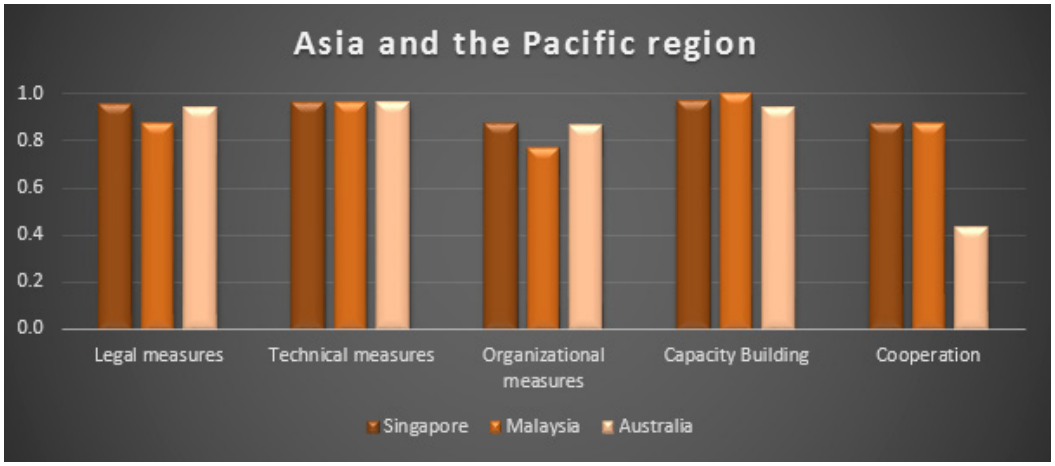
Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Australia	0.82	0.94	0.96	0.86	0.94	0.44

Singapore is the top ranked country in the region. The island state has a long history of cybersecurity initiatives. It launched its first cybersecurity master plan back in 2005. The Cyber Security Agency of Singapore was created in 2015 as a dedicated entity to oversee cybersecurity and the country issued a comprehensive strategy in 2016[8].

Malaysia is ranked second in the Asia and the Pacific region and scores a perfect 100 on capacity building due to a range of initiatives in that pillar. Cybersecurity Malaysia, the government entity responsible for information security in the country, offers professional training via higher education institutions in Malaysia. It maintains the *Cyberguru* website, dedicated to professional security training[9].

Australia[10] is third ranked in the region and home to AusCERT, one of oldest CERTs in the region formed in 1993[11]. The highest scoring pillar is technical where there is a certification programme for information security skills provided by the Council of Registered Ethical Security Testers (CREST)[12]. Modelled after CREST, the council offers assessment, accreditation, certification, education and training in cyber and information security for individuals and corporate entities in both Australia and New Zealand.

Figure 6.4.1: Top three ranked countries and an average score of all Asia and the Pacific



8 https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy
9 http://www.cyberguru.my
10 http://thecommonwealth.org/member-countries
11 https://www.auscert.org.au
12 https://www.crestaustralia.org

Figure 6.4.2: Asia and the Pacific Region Scorecard

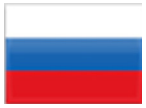
	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURES**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURES**	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	**COOPERATION**	**GCI**
Afghanistan	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🟡	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴
Australia	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🔴	🟢	🟡	🟢
Bangladesh	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🔴	🟢	🔴	🟡	🟢	🔴	🟢	🟢	🟡	🟡	🟢	🔴	🟡	🔴	🔴	🟢	🟡	🔴	🔴	🟡
Bhutan	🔴	🔴	🔴	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🟢	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Brunei Darussalam	🟢	🔴	🟢	🟡	🟢	🟢	🔴	🔴	🔴	🟢	🟡	🟢	🟡	🔴	🟡	🔴	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟡
Cambodia	🟡	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🟢	🔴	🟡	🟢	🔴	🔴	🔴	🟡	🟡	🔴	🟢	🔴	🔴	🔴	🔴
China	🟡	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🔴	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🔴	🔴	🟢	🟡
Democratic People	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🔴	🟢	🔴	🟡	🟡	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🟢	🟡
Fiji	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🔴	🔴	🔴
India	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🟢	🟢	🔴	🔴	🟡	🟢
Indonesia	🟢	🟡	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🟡	🟢	🟢	🔴	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🟢	🔴	🟡
Iran	🟢	🟡	🔴	🟡	🟡	🟢	🟢	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟡	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟡
Japan	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟡	🟢	🟢	🔴	🟢	🟢	🟢
Kiribati	🟢	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Lao	🟢	🟡	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟡	🟡
Malaysia	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢
Maldives	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Marshall Islands	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Micronesia	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Mongolia	🔴	🟡	🔴	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🔴	🔴
Myanmar	🟡	🟡	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴
Nauru	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴
Nepal	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴
New Zealand	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟡	🟢	🟢	🟡	🟡	🟢	🟡	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢
Pakistan	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🟡
Palau	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Papua New Guinea	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Philippines	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🔴	🔴	🟢	🟡	🟢	🟢	🔴	🟡	🟡	🟢	🟡	🟡	🟢	🟡	🔴	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🟡	🟡
Republic of Korea	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢
Samoa	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Singapore	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Solomon Islands	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Sri Lanka	🔴	🔴	🟢	🔴	🟢	🟢	🟢	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🟢	🟡	🟢	🟢	🟡	🔴	🔴	🟡	🔴	🟢	🟢	🟡	🔴	🟡	🟡
Thailand	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🟡	🔴	🟡	🟢
Timor-Leste	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Tonga	🟢	🔴	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🟡	🟢	🟡	🔴
Tuvalu	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Vanuatu	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🔴	🔴
Viet Nam	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴

6.5 Commonwealth of Independent States

Table 6.5.1: Top three ranked countries in Commonwealth of Independent States

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Georgia	0.81	0.91	0.77	0.82	0.9	0.7
Russian Federation	0.78	0.82	0.67	0.85	0.91	0.7
Belarus	0.59	0.85	0.63	0.33	0.68	0.47

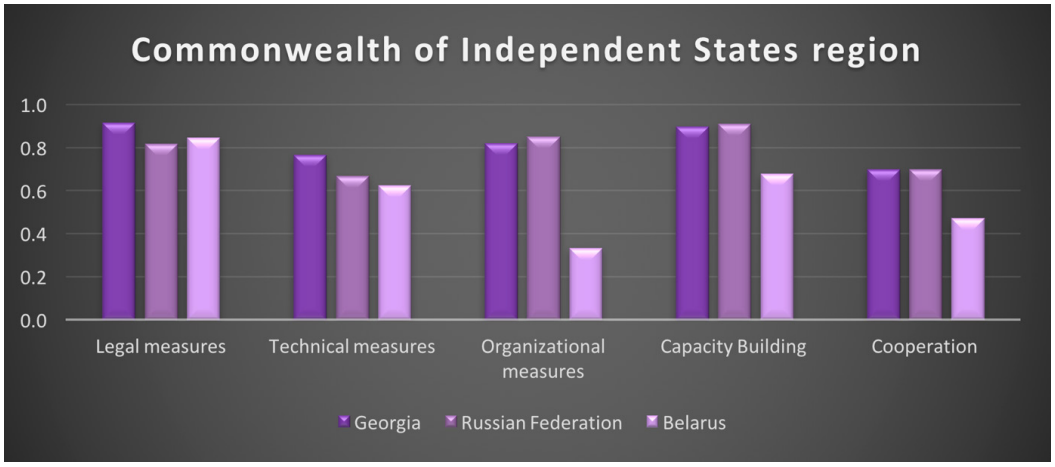
Georgia is top ranked in the CIS. After large-scale cyber-attacks on the country in 2008, the government has strongly supported protection of the country's information systems[13]. The Information Security Law[14] established a Cyber Security Bureau with a particular emphasis on protecting critical information systems in the military sphere.



The Russian Federation, ranked second in the region, scores best in capacity building. Its commitments range from developing cybersecurity standards to R&D and from public awareness to a home-grown cybersecurity industry. An example of the latter is Kaspersky Labs, founded in 1997 and whose software protects over 400 million users and some 270 000 organizations[15].

Belarus is the third ranked country, where child protection initiatives include public and private partnerships. Mobile operator MTS has implemented a project with the Ministry of Education to teach children about safe Internet practices that has so far reached some 6 000 children[16].

Figure 6.5.1: Top three ranked countries and an average score of all CIS



[13] http://www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept.aspx?lang=en-US
[14] https://matsne.gov.ge/en/document/view/1679424
[15] https://usa.kaspersky.com/about
[16] http://www.mts.by/news/97338/

Figure 6.5.2: CIS region scorecard

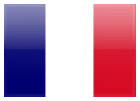
	Cybercriminal le	Cybersecurity le	Cybersecurity t	**LEGAL MEA**	National CERT/CI	Government CERT/C	Sectoral CERT/CII	Standards for orga	Standards for prof	Child online pro	**TECHNICAL ME**	Strate	Responsible :	Cybersecurity	**ORGANIZATIONAL I**	Standardizatior	Cybersecurity good	R&D progra	Public awareness c	Professional trainin	Education progr	Incentive mect	Home-grown ii	**CAPACITY BU**	Bilateral agree	Multilateral agre	International part	Public-private par	Interagency part	**COOPERA**	**Gl**
Armenia	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Azerbaijan	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟡	🟡	🔴	🔴	🟡	🟢	🟡	🟢	🟢	🟡	🔴	🔴	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟡
Belarus	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟢	🟢	🔴	🟢	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🟢	🟡	🟢	🔴	🟢	🟡	🟡
Georgia	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢
Kazakhstan	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🔴	🟡	🔴	🔴	🟡	🔴	🟡	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Moldova	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🔴	🟡	🔴	🟢	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🟡	🟢	🟡	🟡
Russian Federation	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢
Tajikistan	🟡	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🟡	🔴	🟢	🟡	🟡	🔴	🟡	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Turkmenistan	🟡	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Ukraine	🟡	🟢	🟢	🟢	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟢	🔴	🔴	🟡	🟡	🟡	🔴	🔴	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟡
Uzbekistan	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴

6.6 Europe

Table 6.6.1: Top three ranked countries in Europe

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
France	0.81	0.94	0.96	0.6	1	0.61
Norway	0.78	0.96	0.89	0.64	80.8	0.57

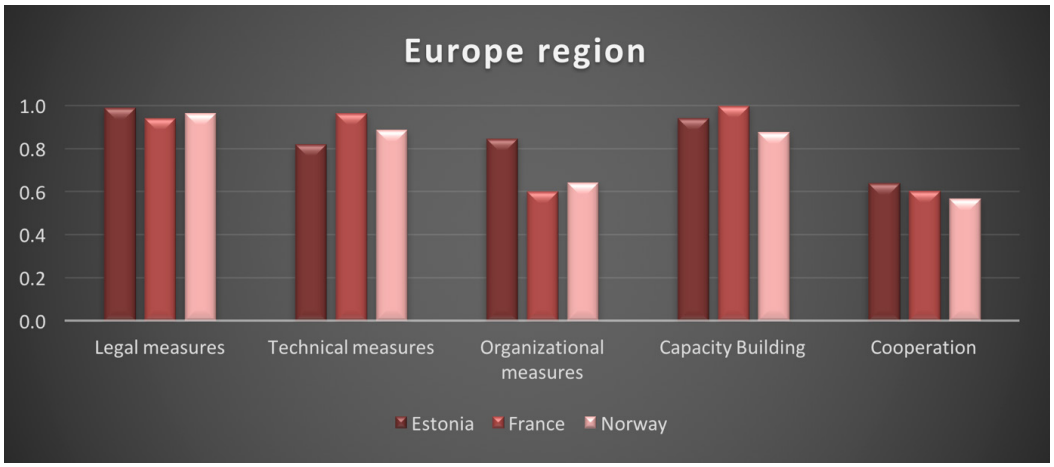
Estonia is the highest-ranking nation in the Europe region. Like Georgia, Estonia enhanced its cybersecurity commitment after a 2007 attack. This included the introduction of an organizational structure that can respond quickly to attacks as well as a legal act that requires all vital services to maintain a minimal level of operation if they are cut off from the Internet[17]. The country also hosts the headquarters of the NATO Cooperative Cyber Defence Centre of Excellence[18].



France is the second highest ranked in the Europe region, scoring a perfect 100 in capacity building. There is widespread cybersecurity training available in the country, and the National Agency for Information System Security (ANSSI in French) publishes a list of dozens of universities that provide accredited cybersecurity degrees recognized[19].

Norway is ranked third in Europe with its highest score in the legal pillar. Apart from laws dealing with cybersecurity, Norway has also conducted research on its cybersecurity culture including surveying citizens about the degree to which they will accept monitoring of their online activities.[20]

Figure 6.6.1: Top three ranked countries and an average score of all Europe



[17] http://www.nextgov.com/cybersecurity/2015/01/heres-what-us-could-learn-estonia-about-cybersecurity/103959/
[18] https://ccdcoe.org
[19] https://www.ssi.gouv.fr/particulier/formations/formation-et-cybersecurite-en-france/
[20] https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf

Figure 6.6.2: Europe region scorecard

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURES**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURES**	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	**COOPERATION**	**GCI**
Albania	🔴	🟡	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟢	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟢	🟡	🔴
Andorra	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Austria	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🟢	🔴	🟡	🟡	🔴	🟢	🟢	🟡	🟢	🟡	🟡	🟡	🔴	🟢	🔴	🟢	🟢	🟡	🟢
Belgium	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🔴	🟢	🟢	🟡	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟢
Bosnia and Herzegovina	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴
Bulgaria	🔴	🟢	🟢	🟡	🟢	🟢	🔴	🟡	🔴	🟢	🟡	🔴	🟡	🟢	🟡	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🟡	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟡
Croatia	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟡	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🔴	🟢	🔴	🟢	🟢	🟢	🟡	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟢
Cyprus	🔴	🟡	🟢	🟡	🔴	🟢	🟢	🔴	🔴	🟢	🟡	🟢	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🟡	🟢	🔴	🟡	🟡	🔴	🟢	🟢	🟡	🔴	🟡	🟡
Czech Republic	🟡	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟢	🔴	🔴	🟢	🟡	🔴	🔴	🟢
Denmark	🔴	🟢	🔴	🔴	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🔴	🟢	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Estonia	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢
Finland	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟡	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢
France	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🔴	🟢	🟡	🟢	🟢	🟢
Germany	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🟢	🔴	🟢	🟢	🟢	🟡	🟡	🟡	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟢
Greece	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟡	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🔴	🔴	🟡
Hungary	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟢	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🟢	🟡	🟡	🔴	🟡	🔴	🔴	🟢	🟢	🔴	🟢	🟡	🟡
Iceland	🟡	🟡	🟡	🟡	🟡	🔴	🟢	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🟡	🔴	🟡	🟡
Ireland	🟡	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Israel	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢
Italy	🔴	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🟢	🟢	🟡	🟢	🟡	🟢	🔴	🟢	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Latvia	🟢	🟡	🟡	🟡	🟢	🔴	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🔴	🟡	🟢	🟢	🟡	🟢	🟡	🟡	🟡	🟡	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢
Liechtenstein	🟢	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Lithuania	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🔴	🟢	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🟡	🔴	🟢	🟡	🔴	🟡	🟢
Luxembourg	🟡	🟢	🟡	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🟢	🟡	🟢	🟡	🟡	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🟢	🟡	🔴	🔴	🟢	🟡	🟢	🟡	🟢
Malta	🔴	🟢	🔴	🔴	🟡	🟢	🟢	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🟡	🟢	🟡	🔴	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Monaco	🟡	🟢	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Montenegro	🔴	🟡	🔴	🔴	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🟢	🟡	🟡	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🟡
Netherlands	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢	🟡	🟢	🟢	🟢	🟡	🔴	🟢	🟢	🟢	🟡	🟡	🟡	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢
Norway	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢
Poland	🟢	🟢	🔴	🟡	🟡	🟢	🟢	🟡	🟡	🟢	🟡	🟡	🟡	🟡	🟢	🟡	🟢	🟡	🟢	🟡	🟢	🔴	🟡	🟡	🟡	🔴	🟢	🟢	🟢	🟢	🟢
Portugal	🟡	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🟢	🟢	🟢	🟡	🟡	🟡	🔴	🔴	🟢	🔴	🟢	🟡	🟡
Romania	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟡	🟢	🔴	🟡	🟢	🔴	🔴	🟢	🟡	🟡	🔴	🔴	🟡	🟡	🔴	🟢	🟢	🟢	🟢	🟡
San Marino	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Serbia	🟢	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟢	🟡	🔴	🟢	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟢	🟡	🔴	🔴	🔴
Slovakia	🟡	🔴	🔴	🔴	🟢	🟢	🟢	🟡	🔴	🔴	🟡	🟡	🟢	🟢	🟡	🟡	🔴	🔴	🔴	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Slovenia	🔴	🔴	🔴	🔴	🟢	🟢	🟢	🔴	🔴	🟡	🟡	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🟡
Spain	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟡	🟡	🟢	🔴	🟡	🟡	🔴	🟡	🟢	🔴	🟢	🟢	🟡	🟡	🟢	🔴	🟢	🔴	🔴	🟡	🟡
Sweden	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🟢	🟢	🟡	🔴	🔴	🟢	🟢	🟢	🟢	🟢
Switzerland	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🔴	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟢	🟢
The former Yugoslav Republic of Macedonia	🔴	🟢	🔴	🔴	🔴	🟢	🟢	🔴	🔴	🟡	🔴	🔴	🟢	🔴	🟡	🟡	🟢	🟢	🟢	🟢	🟡	🟡	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟡
Turkey	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟡	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🟡
United Kingdom	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🔴	🔴	🟢	🟢	🔴	🟡	🟢

7 Illustrative practices by pillar

This chapter identifies noteworthy and thought-provoking practices in cybersecurity across the various GCI pillars. Examples are drawn from a number of countries and provide an insight on the cybersecurity commitment taken in their focus areas.

7.1 Legal

Examples for this pillar illustrate practices in national cybercrime legislation regarding unauthorized access, data and system interference or interception, and misuse of computer systems.

7.1.1 Cybercrime legislation

Colombia became one of the first countries in the world when, in 2009, it enacted a law specifically targeting cyberspace. Law 1273 (entitled "By means of which the Penal Code is amended, a new legal right is created- called 'protection of information and data'- and systems that use information and communication technologies are fully preserved, among other provisions"[1]) calls for a prison sentence or large fines for anyone convicted of information systems or telecommunication network crimes. The law covers areas such as illegally accessing personal information, intercepting data, destroying data or using malicious software.

Georgia established cybercrime legislation in line with the principles and rules of the Budapest Convention both in terms of substantive and procedural aspects. Illegal access to information systems, data and system interference, and misuse of devices are criminalized by the Georgia criminal code. The Personal Data Protection Act was enacted by Parliament in 2011 and is intended to ensure protection of human rights and freedoms, including the right to privacy, in the course of personal data processing.[2]

7.1.2 Cybersecurity regulation

Sultanate of Oman established the eGovernance Framework, a set of standards / best practices and process management systems to enhance the delivery of government services in alignment with the mission of e.oman (Sultanate of Oman Digital Oman Strategy and eGovernment). The framework spells out the rules and procedures that ensure that government IT projects and systems are sustainable and in compliance with the Information Technology Authority (ITA) strategies and objectives. It provides assurance about the value of IT projects and framework for the management of IT-related risks. It helps in putting controls to minimize risks and better delivery of IT initiatives[3].

7.1.3 Cybersecurity training

Mauritius makes available training for law enforcement and judiciary which has been conducted under the GLACY Project since 2013 and is still ongoing. CERT-MU also carried out cybersecurity trainings on digital forensic investigator professional and network forensic (packet analysis) for law enforcement officers. Training on

---

1 Government of Colombia. Law 1273 of 2009. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. http://www.mintic.gov.co/portal/604/w3-article-3705.html

2 https://personaldata.ge/en/legislation/national-legislation ; https://matsne.gov.ge/ka/document/view/16426?impose=translateEn

3 http://www.ita.gov.om/ITAPortal/Government/Government_Projects.aspx?NID=76

information security standards and best practices is given to the technical officers of the IT Security Unit (ITSU) of the Ministry of Technology, Communication and Innovation[4].

The **New Zealand** (NZ) Police is introducing a 3-tiered training program for specialist cyber staff, investigators and then frontline staff. This is outlined in NZ Police's Prevention First National Cybercrime Strategy 2014-2017[5]. NZ Police also provides training to the judiciary and prosecutors.

7.2 Technical

Examples for this pillar illustrate practices in areas such as existence of technical institutions, child online protection and industry standards and certification.

7.2.1 National CERT/CIRT/CSIRT

Egypt provides computer emergency response team (EG-CERT) support to several entities in the ICT sector, the financial sector as well as the government sector, in order to help them tackle cybersecurity related threats. EG-CERT is expanding and is currently upgrading its laboratories in the four key operational departments. Additional laboratories are being planned for mobile cybersecurity and industrial control systems cybersecurity[6].

Brazil has three computer emergency response teams with different functions, namely: the national CERT, a government CSIRT and a sector specific SCIRT. The Brazil Federal Police participates in the I-24/7 global police communications system developed by Interpol to connect law enforcement officers, including cybercrimes. There is also a complementary Standard No. 17/IN01/DSIC/GSIPR that establishes guidelines for the certification and accreditation for information and communication security professionals of the direct and indirect Federal Public Administration.

7.2.2 Government CERT/CIRT/CSIRT

Luxembourg created a computer emergency response team (GOVCERT.LU) in 2011 to help protect government computer systems and data as well as specific infrastructures and is engaged at both national and international level under the name of NCERT.LU[7]. GOVCERT.LU is also a critical player in the event of a large cyber-attack affecting country's ICT assets.

7.2.3 Sectoral CERT/CIRT/CSIRT

Sri Lanka created the Financial Sector Computer Security Incident Response Team (FINCSIRT) in 2014 with responsibility for receiving, reviewing, processing and responding to computer security alerts and incidents affecting banks and other licensed financial institutions in the country[8]. FINCSIRT is a joint initiative of the Central Bank of Sri Lanka and the Sri Lanka computer emergency response team and is steered and funded by the banking sector. Related to FINCSIRT is LankaClear, the country's certification authority owned by the Central Bank and commercial banks[9].

---

4 http://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/glacy-support-to-mauritius-judicial-training-courses-on-cybercrime-delivered
5 http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-cybercrime-plan-december-2015.pdf (page 10)
6 http://www.egcert.org
7 https://www.govcert.lu/en/ncert.html
8 http://www.fincsirt.lk
9 http://www.lankaclear.com/about/index.php

7.2.4 Cybersecurity standards implementation framework for organizations

Malaysia created the Information Security Certification Body (ISCB), a department of Cybersecurity Malaysia, which manages information security certification[10]. The certification services are consistent with international standards and guidelines and include among others the Malaysian Common Criteria Evaluation and Certification (MyCC), which certifies security functions of ICT products based on the ISO/IEC 15408 international standard[11].

Hungary national regulation lays out the framework for information security training for state and local government officials[12]. The National University for Public Service (NKE) is charged with training and establishing a certification system[13]. Certificates issued include information security risk assessment and testing of electronic information systems.

7.2.5 Child online protection

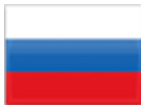
Singapore's Internet Content Providers (ICPs) and Internet Access Service Providers (IASPs) are licensable under the Broadcasting Act and they are required to comply with the Internet Code of Practice to protect children online. Since 2012, all service providers have been legally obligated to offer filtering services with Internet subscriptions and to make this known to consumers when they subscribe or renew. The Info-communications Media Development Authority also symbolically blocks 100 pornographic, extremist or hate websites.

7.3 Organizational

Examples for this pillar illustrate practices where governments are organized by having a cybersecurity strategy, a coordinating agency and compilation of indicators for tracking cybercrime.

7.3.1 Strategy

United Kingdom issued in 2016 its second five years *National Cyber Security Strategy*[14]. The strategy, issued by the Cabinet Office, aims to make the country one of the safest places in the world to carry out online business and doubles investment in cybersecurity compared to the first plan.



Russian Federation officially adopted its National Security Strategy in 2000 and National Security Concept of the Russian Federation as well as Concept of the Foreign Policy of the Russian Federation in 2013. It established an Information Security Doctrine of the Russian Federation in 2000 and each government entity in the Russian Federation performs an annual audit of its own networks and systems in line with the doctrine and the areas identified in the various strategies adopted.

---

10 http://www.cybersecurity.my/en/our_services/iscb/main/detail/2327/index.html
11 http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341
12 http://njt.hu/cgi_bin/njt_doc.cgi?docid=164331.250717
13 http://en.uni-nke.hu
14 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

7.3.2 Public consultation

Canada conducted a three-month public consultation on updating its cybersecurity strategy, asking security professionals and citizens for inputs and views. The consultation was done to help identify gaps and opportunities, bring forward new ideas to shape Canada's renewed approach to cybersecurity and capitalize on the advantages of new technology and the digital economy[15].

7.3.3 Responsible agency

Iceland created the Cyber Security Council, appointed by the Minister of the Interior that is responsible for overseeing the implementation of the National Cyber Security Strategy. In addition, a cyber security forum has been created as a collaborative venue for representatives of public bodies who sit on the Cyber Security Council and of private entities.

7.3.4 Cybersecurity metrics

Netherlands uses metrics annually in order to measure cybersecurity development at a national level, summarized in the Cyber Security Assessment Netherlands report[16]. The National Cyber Security Centre (NCSC) compiles disclosure reports, security advisories and incidents using a registration system. The metrics allow trends to be observed and acted on.

7.4 Capacity building

Examples of practices for capacity building include the aspects of developing the technical and human resources for fighting cybercrime. This includes raising awareness about cybersecurity among the public, the existence of cybersecurity standards and standards bodies, best practices guides, education initiatives and research and development.

7.4.1 Standardization bodies

Romania created the National Standardization Organization[17] to produce relevant national standards on processes, tools and technologies for software products and systems in the area of security in information technology. It also tests the standardization integrity of encryption algorithms, authentication services and algorithms for confidential services in compliance with accepted international standards[18].

7.4.2 Good practice

Canada created the Investment Industry Regulatory Organization (IIROC) that is the national self-regulatory organization overseeing investment dealers and their trading activity in the country's debt and equity markets. IIROC published a cybersecurity best practices guide for its members[19].

---

15 http://www.itworldcanada.com/article/breaking-news-ottawa-announces-public-consultation-on-cyber-security-strategy/385740#ixzz4dm1QjsTu

16 https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html

17 http://www.asro.ro/

18 http://www.asro.ro/CTmementoSite.html#BM208

19 http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

7.4.3 Cybersecurity research and development programmes

Germany signed an agreement in 2009 on cooperation in IT security research between the Federal Ministry of Education and Research (BMBF) and the Federal Ministry of the Interior (BMI). The IT Security Research programme covers research and development in new information security technologies. The BMBF has been supporting three research centres since 2011 that bring together leading university and non-university establishments in cybersecurity[20].

Kenya Education Network, (KENET), is the National Research and Education Network (NREN) of Kenya. KENET is the computer emergency response team (CERT) for the academic community and is licensed by the Communications Authority of Kenya (CA) as a not-for-profit operator serving the education and research institutions. They most notably provide affordable, cost-effective and low-congestion Internet bandwidth services to member institution campuses in Kenya.

7.4.4 Public awareness campaigns

Latvia has published a series of articles on its national CERT portal about free-of-charge security solutions including anti-viruses, firewalls, NoScript, etc.[21] Twice a year, the national CERT organizes a campaign where people can bring their computers for a check-up to see if they are infected, and it also distributes commercial anti-virus installations during the campaigns that are made available free-of-charge for one year.

7.4.5 Cybersecurity professional training courses

Bulgaria established the International Cyber Investigation Training Academy in 2009, which is a non-governmental organization[22]. The academy aims to improve the qualification of specialists working in the field of cybersecurity. It has trained over 1 300 people from both the public and private sectors.

7.4.6 National education programmes and academic curricula

Germany has several universities and institutes providing degrees and certificates in information security[23]. The Federal Ministry of Education and Research funds the KASTEL competence centre that offers training leading to a certificate equivalent to a specialized master degree in IT security[24]. The Technical University of Darmstadt has been offering a Master of Science Degree in IT security since 2010[25].

7.4.7 Incentive mechanisms

Korea Internet Security Agency (KISA) is committed to establishing a network foundation for Internet users and Internet companies by improving competitiveness of Internet services and reliability of Internet information and knowledge. KISA supports start-ups to commercialize their business models and enhance competitive edge in the field of security technology through programmes that aim to nurture start-ups in the Internet-of-things, security, and Fintech industry. They also established the one-stop

[20] https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html
[21] https://www.esidross.lv/category/bezmaksas-risinajumi/page/2/
[22] http://e-crimeacademy.com/
[23] https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html
[24] http://www.kastel.kit.edu
[25] https://www.tu-darmstadt.de/studieren/abschluesse/master/it-sicherheit-msc.en.jsp

service to support start-ups to gain ground not only in the domestic market but also the global market to expand their business models.

7.4.8 Home-grown cybersecurity industry

Ireland has the largest proportion of the Information and Communication sector of its economy compared to all other countries in Europe and is leveraging that advantage to grow its cybersecurity industry. The country is drawing on existing incentives and attractions with the aim of being a cybersecurity capital[26]. These incentives include a favourable business environment and low taxes, a talented pool of highly skilled and multilingual workers and a good base for access to European markets[27].

7.5 Cooperation

This pillar considers collaborative efforts across national and international domains and between the public and private sector.

7.5.1 Bilateral agreements

Finland is an active member of many organizations, such as the Council of Europe (CoE), the Organization for Security and Co-operation in Europe (OSCE) and the United Nations (UN). Finland has also joined the NATO Partnership for Peace and is engaged in cooperation with the organization in, for example, crisis management. There is also local partnership with Finnish company Codenomicon, which later was acquired by Synopsys, to develop the national IDS system and automatic incident reporting service with FICORA[28].

7.5.2 Multilateral agreements

Denmark, Finland, Iceland, Norway and **Sweden** collaborate through the Nordic National CERT Collaboration. This includes technical cooperation and cybersecurity exercises to assess and strengthen cyber preparedness, examine incident response processes and enhance information sharing in the region[29].

7.5.3 Participation in international fora

Participation in international cybersecurity events, workshops and training is the one indicator where virtually all countries score high on the GCI. Therefore, it is more revealing to describe one of the most significant initiatives in this regard. The Forum of Incident Response and Security Teams (FIRST)[30] was founded in 1990. Its members are security and incident response teams from the public, private and academic sectors. It organizes an annual conference, technical colloquia and training workshops.

---

26 https://www.siliconrepublic.com/companies/cybersecurity-hub-ireland
27 http://www.idaireland.com/how-we-help/resources/infographics/ida-cyber-security/IDA_CYBER_SECURITY.pdf
28 http://formin.finland.fi/public/default.aspx?nodeid=49303&contentlan=2&culture=fi-FI https://www.synopsys.com/services.html
29 https://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/
30 www.FIRST.org

7.5.4 Public -private partnerships

The **United Kingdom** is working with local company Netcraft on cyber security initiatives.[31] This includes combatting phishing and malware hosted in the United Kingdom as well as phishing targeting the government[32]. The partnership helped stop 34,550 potential attacks on government departments in the last six months of 2016, or 200 incidents a day.

7.5.5 Interagency partnerships

The **United States of America** started its first cross-government security information sharing agreement in 2015. The Multilateral Information Sharing Agreement (MISA) binds government agencies from defence, health, justice, intelligence community and energy to work collaboratively to enhance cybersecurity information sharing, with an emphasis on information exchanges at machine speed[33].

South Africa established the national cybersecurity hub to serve as a central point for collaboration between industry, government and civil society on all cybersecurity incidents. The cybersecurity hub is mandated by the National Cybersecurity Policy Framework (NCPF) that was passed by Cabinet in 2012. The hub enhances interaction and consultations as well as promoting a coordinated approach regarding engagements with the private sector and civil society[34].

[31] https://news.netcraft.com/archives/2016/11/01/the-chancellor-of-the-exchequer-sets-out-plans-for-the-uk-government-to-work-with-netcraft.html
[32] https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk
[33] https://www.ise.gov/blog/kshemendra-paul/coordinating-cybersecurity-programs
[34] https://www.cybersecurityhub.gov.za/

8 Conclusion

Cybersecurity is an increasingly important part of our life today, and the degree of interconnectivity of networks implies that anything and everything can be exposed, and everything from national critical infrastructure to our basic human rights can be compromised. Governments are therefore urged to consider policies that support continued growth in technology sophistication, access and security, and as a crucial first step, to adopt a national cybersecurity strategy.

The GCI 2017 edition measured the commitment of the ITU Member States to cybersecurity and highlighted a number of illustrative practices from around the world. As a logical continuation of the first iteration of the GCI issued in 2014, this version has motivated countries to improve their work related to cybersecurity, raised awareness in countries for the need to start bilateral, multilateral and international cooperation, and increased the visibility of what countries are doing to improve cybersecurity.

However, the research also revealed that while increased Internet access and more mature technological development is correlated with improvement in cybersecurity at the global level, this is not necessarily true for countries with developing economies and lower levels of technological development. The data collection shows that developing countries lack well-trained cybersecurity experts as well as a thorough appreciation and the necessary education on cybersecurity issues for law enforcement, and continued challenges in the judiciary and legislative branches. There is a need for the developed world to help train local experts in cybersecurity, and more cooperation should be initiated between developed and developing countries to assist them in cybersecurity development.

For the Global Cybersecurity Index to have an impact on raising awareness on this crucial emerging concern over time, continuity of the GCI effort is essential. ITU therefore welcomes all Member States and industry stakeholders to actively participate in future efforts to enhance the current reference model. As well, the success of future iterations of the GCI largely depends on the engagement of Member States and the quality of their responses to the questionnaire, and ITU calls on all Member States to take part in the next GCI survey.

ITU would like to thank all Member States for their valuable support for the conduct of the GCI survey and the publication of this report as well as future ones.

Abbreviations

CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CIIP	Critical Information Infrastructure Protection
CIS	Commonwealth of Independent States
CREST	Council of Registered Ethical Security Testers
CSIRT	Computer Security Incident Response Team
COP	Child Online Protection
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
GOVCERT	Governmental Computer Emergency Response Team
GCI	Global Cybersecurity Index
ICT	Information and Communication Technology
ITU	International Telecommunication Union
ISP	Internet Service Provider
NCS	National Cybersecurity Strategy
UN	United Nations
R&D	Research and Development
NATO	North Atlantic Treaty Organization
NAFTA	North American Free Trade Association
PIPEDA	Personal Information Protection and Electronic Documents Act
ANSSI	National Agency for Information System Security
ISCB	Information Security Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification
MTPS	Malaysia Trustmark for Private Sector
NCSC	The National Cyber Security Centre
BMBF	Federal Ministry of Education and Research
ISACA	Information Systems Audit and Control Association
ICP	Internet Content Provider
IASPs	Internet Access Service Provider
NCSC	Nation Cyber Security Centre
MSIP	Ministry of Science, ICT and Future Planning

IDI	ICT Development Index
GDP	Gross Domestic Product
FINCSIRT	Financial Sector Computer Security Incident Response Team
KISA	Korea Internet and Security Agency
IIROC	The Investment Industry Regulatory Organization of Canada
CERT-MU	Computer Emergency Response Team of Mauritius
National KE-CIRT/CC	National Kenya Computer Incident Response Team Coordination Centre
AfricaCERT	Computer Emergency Response Team of Africa
AusCERT	Computer Emergency Response Team of Australia
GOVCERT.LU	Government Computer Emergency Response Team of Luxembourg
NCERT.LU	National Computer Emergency Response Team of Luxembourg
OCERT	Oman Computer Emergency Response Team
APCERT	Asia and the Pacific Computer Emergency Response Team

Annex 1 – ITU Member States Global Cybersecurity Commitment Score By Region

AFRICA Region	Score	Global Rank
Mauritius	0.830	6
Rwanda	0.602	36
Kenya	0.574	45
Nigeria	0.569	46
Uganda	0.536	50
South Africa	0.502	58
Botswana	0.430	69
Côte d'Ivoire	0.416	74
Cameroon	0.413	75
Ghana	0.326	87
Tanzania	0.317	88
Senegal	0.314	89
Zambia	0.292	91
Ethiopia	0.267	99
Togo	0.218	107
Burkina Faso	0.208	108
Mozambique	0.206	109
Zimbabwe	0.192	113
Seychelles	0.184	115
Niger	0.170	120
Madagascar	0.168	121
Liberia	0.149	124
Sierra Leone	0.145	126
Gabon	0.139	128
Gambia	0.136	130
Burundi	0.120	135
Lesotho	0.094	143
Guinea	0.090	144

AFRICA Region	Score	Global Rank
Malawi	0.084	145
Angola	0.078	146
Eritrea	0.076	147
Chad	0.072	148
Benin	0.069	149
South Sudan	0.067	150
Namibia	0.066	151
Mali	0.060	152
Cape Verde	0.058	153
Swaziland	0.041	160
Congo	0.040	161
Democratic Republic of the Congo	0.040	161
Sao Tome and Principe	0.040	161
Guinea-Bissau	0.034	162
Central African Republic	0.007	164
Equatorial Guinea	0.000	165

AMERICAS Region	Score	Global Rank
United States of America	0.919	2
Canada	0.818	9
Mexico	0.660	28
Uruguay	0.647	29
Brazil	0.593	38
Colombia	0.569	46
Panama	0.485	62
Argentina	0.482	63
Ecuador	0.466	66
Peru	0.374	79
Venezuela	0.372	80
Chile	0.367	81

AMERICAS Region	Score	Global Rank
Jamaica	0.339	85
Costa Rica	0.336	86
Paraguay	0.326	87
Barbados	0.273	95
Guyana	0.269	98
El Salvador	0.208	108
Saint Vincent and the Grenadines	0.189	114
Belize	0.182	116
Antigua and Barbuda	0.179	117
Dominican Republic	0.162	122
Suriname	0.155	132
Nicaragua	0.146	125
Bahamas	0.137	129
Bolivia	0.122	134
Grenada	0.115	137
Guatemala	0.114	138
Trinidad and Tobago	0.098	141
Saint Kitts and Nevis	0.066	151
Cuba	0.058	153
Saint Lucia	0.053	156
Honduras	0.048	157
Haiti	0.040	161
Dominica	0.010	163

ARAB STATES Region	Score	Global Rank
Oman	0.871	4
Egypt	0.772	14
Qatar	0.676	25
Tunisia	0.591	40
Saudi Arabia	0.569	46

ARAB STATES Region	Score	Global Rank
United Arab Emirates	0.566	47
Morocco	0.541	49
Bahrain	0.467	65
Algeria	0.432	68
Jordan	0.277	93
Sudan	0.271	96
Syrian Arab Republic	0.237	102
State of Palestine	0.228	104
Libya	0.224	105
Lebanon	0.172	119
Mauritania	0.146	125
Kuwait	0.104	139
Djibouti	0.099	140
Iraq	0.043	159
Comoros	0.040	161
Somalia	0.034	162
Yemen	0.007	164

COMMONWEALTH OF INDEPENDANT STATESCIS Region	Score	Global Rank
Georgia	0.819	8
Russian Federation	0.788	10
Belarus	0.592	39
Azerbaijan	0.559	48
Ukraine	0.501	59
Moldova	0.418	73
Kazakhstan	0.352	83
Tajikistan	0.292	91
Uzbekistan	0.277	93
Kyrgyzstan	0.270	97
Armenia	0.196	111
Turkmenistan	0.133	132

ASIA AND THE PACIFIC Region	Score	Global Rank
Singapore	0.925	1
Malaysia	0.893	3
Australia	0.824	7
Japan	0.786	11
Republic of Korea	0.782	13
New Zealand	0.718	19
Thailand	0.684	20
India	0.683	23
China	0.624	32
Philippines	0.594	37
Democratic People's Republic of Korea	0.532	52
Brunei Darussalam	0.524	53
Bangladesh	0.524	53
Iran	0.494	60
Pakistan	0.447	67
Indonesia	0.424	70
Sri Lanka	0.419	72
Lao	0.392	77
Tonga	0.292	91
Cambodia	0.283	92
Nepal	0.275	94
Myanmar	0.263	100
Viet Nam	0.245	101
Afghanistan	0.245	101
Mongolia	0.228	104
Fiji	0.222	106
Bhutan	0.199	110
Nauru	0.140	127
Vanuatu	0.134	131
Kiribati	0.123	133
Solomon Islands	0.095	142

ASIA AND THE PACIFIC Region	Score	Global Rank
Papua New Guinea	0.067	150
Maldives	0.056	155
Palau	0.053	156
Samoa	0.048	157
Marshall Islands	0.048	157
Micronesia	0.044	158
Timor-Leste	0.034	162
Tuvalu	0.034	162

EUROPE Region	Score	Global Rank
Estonia	0.846	5
France	0.819	8
Norway	0.786	11
United Kingdom of Great Britain and Northern Ireland	0.783	12
Netherlands	0.760	15
Finland	0.741	16
Sweden	0.733	17
Switzerland	0.727	18
Israel	0.691	20
Latvia	0.688	21
Germany	0.679	24
Ireland	0.675	26
Belgium	0.671	27
Austria	0.639	30
Italy	0.626	31
Poland	0.622	33
Denmark	0.617	34
Czech Republic	0.609	35
Luxembourg	0.602	36
Croatia	0.590	41

EUROPE Region	Score	Global Rank
Romania	0.585	42
Turkey	0.581	43
Bulgaria	0.579	44
Hungary	0.534	51
Spain	0.519	54
The Former Yugoslav Republic of Macedonia	0.517	55
Portugal	0.508	56
Lithuania	0.504	57
Cyprus	0.487	61
Greece	0.475	64
Montenegro	0.422	71
Malta	0.399	76
Iceland	0.384	78
Slovakia	0.362	82
Slovenia	0.343	84
Albania	0.314	89
Serbia	0.311	90
Monaco	0.236	103
Liechtenstein	0.194	112
San Marino	0.174	118
Bosnia and Herzegovina	0.116	136
Andorra	0.057	154
Vatican	0.040	161

Annex 2 – GCI 2017 Score

Member State	Score	Global Rank
Singapore	0.925	1
United States of America	0.919	2
Malaysia	0.893	3
Oman	0.871	4
Estonia	0.846	5
Mauritius	0.830	6
Australia	0.824	7
Georgia	0.819	8
France	0.819	8
Canada	0.818	9
Russian Federation	0.788	10
Japan	0.786	11
Norway	0.786	11
United Kingdom	0.783	12
Republic of Korea	0.782	13
Egypt	0.772	14
Netherlands	0.760	15
Finland	0.741	16
Sweden	0.733	17
Switzerland	0.727	18
New Zealand	0.718	19
Israel	0.691	20
Latvia	0.688	21
Thailand	0.684	20
India	0.683	23
Germany	0.679	24
Qatar	0.676	25
Ireland	0.675	26
Belgium	0.671	27

Member State	Score	Global Rank
Mexico	0.660	28
Uruguay	0.647	29
Austria	0.639	30
Italy	0.626	31
China	0.624	32
Poland	0.622	33
Denmark	0.617	34
Czech Republic	0.609	35
Rwanda	0.602	36
Luxembourg	0.602	36
Philippines	0.594	37
Brazil	0.593	38
Belarus	0.592	39
Tunisia	0.591	40
Croatia	0.590	41
Romania	0.585	42
Turkey	0.581	43
Bulgaria	0.579	44
Kenya	0.574	45
Colombia	0.569	46
Saudi Arabia	0.569	46
Nigeria	0.569	46
United Arab Emirates	0.566	47
Azerbaijan	0.559	48
Morocco	0.541	49
Uganda	0.536	50
Hungary	0.534	51
Democratic People's Republic of Korea	0.532	52
Brunei Darussalam	0.524	53
Bangladesh	0.524	53
Spain	0.519	54

Member State	Score	Global Rank
The Former Yugoslav Republic of Macedonia	0.517	55
Portugal	0.508	56
Lithuania	0.504	57
South Africa	0.502	58
Ukraine	0.501	59
Iran	0.494	60
Cyprus	0.487	61
Panama	0.485	62
Argentina	0.482	63
Greece	0.475	64
Bahrain	0.467	65
Ecuador	0.466	66
Pakistan	0.447	67
Algeria	0.432	68
Botswana	0.430	69
Indonesia	0.424	70
Montenegro	0.422	71
Sri Lanka	0.419	72
Moldova	0.418	73
Côte d'Ivoire	0.416	74
Cameroon	0.413	75
Malta	0.399	76
Lao	0.392	77
Iceland	0.384	78
Peru	0.374	79
Venezuela	0.372	80
Chile	0.367	81
Slovakia	0.362	82
Kazakhstan	0.352	83
Slovenia	0.343	84
Jamaica	0.339	85

Member State	Score	Global Rank
Costa Rica	0.336	86
Ghana	0.326	87
Paraguay	0.326	87
Tanzania	0.317	88
Senegal	0.314	89
Albania	0.314	89
Serbia	0.311	90
Zambia	0.292	91
Tajikistan	0.292	91
Tonga	0.292	91
Cambodia	0.283	92
Uzbekistan	0.277	93
Jordan	0.277	93
Nepal	0.275	94
Barbados	0.273	95
Sudan	0.271	96
Kyrgyzstan	0.270	97
Guyana	0.269	98
Ethiopia	0.267	99
Myanmar	0.263	100
Viet Nam	0.245	101
Afghanistan	0.245	101
Syrian Arab Republic	0.237	102
Monaco	0.236	103
Mongolia	0.228	104
State of Palestine	0.228	104
Libya	0.224	105
Fiji	0.222	106
Togo	0.218	107
Burkina Faso	0.208	108
El Salvador	0.208	108

Member State	Score	Global Rank
Mozambique	0.206	109
Bhutan	0.199	110
Armenia	0.196	111
Liechtenstein	0.194	112
Zimbabwe	0.192	113
Saint Vincent and the Grenadines	0.189	114
Seychelles	0.184	115
Belize	0.182	116
Antigua and Barbuda	0.179	117
San Marino	0.174	118
Lebanon	0.172	119
Niger	0.170	120
Madagascar	0.168	121
Dominican Republic	0.162	122
Suriname	0.155	132
Liberia	0.149	124
Mauritania	0.146	125
Nicaragua	0.146	125
Sierra Leone	0.145	126
Nauru	0.140	127
Gabon	0.139	128
Bahamas	0.137	129
Gambia	0.136	130
Vanuatu	0.134	131
Turkmenistan	0.133	132
Kiribati	0.123	133
Bolivia	0.122	134
Burundi	0.120	135
Bosnia and Herzegovina	0.116	136
Grenada	0.115	137
Guatemala	0.114	138

Member State	Score	Global Rank
Kuwait	0.104	139
Djibouti	0.099	140
Trinidad and Tobago	0.098	141
Solomon Islands	0.095	142
Lesotho	0.094	143
Guinea	0.090	144
Malawi	0.084	145
Angola	0.078	146
Eritrea	0.076	147
Chad	0.072	148
Benin	0.069	149
South Sudan	0.067	150
Papua New Guinea	0.067	150
Saint Kitts and Nevis	0.066	151
Namibia	0.066	151
Mali	0.060	152
Cape Verde	0.058	153
Cuba	0.058	153
Andorra	0.057	154
Maldives	0.056	155
Saint Lucia	0.053	156
Palau	0.053	156
Honduras	0.048	157
Samoa	0.048	157
Marshall Islands	0.048	157
Micronesia	0.044	158
Iraq	0.043	159
Swaziland	0.041	160
Congo	0.040	161
Democratic Republic of the Congo	0.040	161
Haiti	0.040	161

Member State	Score	Global Rank
Sao Tome and Principe	0.040	161
Vatican	0.040	161
Comoros	0.040	161
Guinea-Bissau	0.034	162
Somalia	0.034	162
Timor-Leste	0.034	162
Tuvalu	0.034	162
Dominica	0.010	163
Central African Republic	0.007	164
Yemen	0.007	164
Equatorial Guinea	0.000	165

International Telecommunication Union

Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

ISBN: 978-92-61-25071-3

9 789261 250713

Printed in Switzerland
Geneva, 2017

Photo credits: Shutterstock

Pew Research Center

What Americans Know About Cybersecurity

March 2017

MARCH 22, 2017

What the Public Knows About Cybersecurity

A majority of internet users can answer fewer than half the questions correctly on a difficult knowledge quiz about cybersecurity issues and concepts

BY KENNETH OLMSTEAD (HTTP://WWW.PEWINTERNET.ORG/AUTHOR/KOLMSTEAD/) AND AARON SMITH (HTTP://WWW.PEWRESEARCH.ORG/STAFF/AARON-SMITH/)

> **Before you read the report,** test your cybersecurity knowledge by taking the interactive quiz (http://www.pewinternet.org/quiz/cybersecurity-knowledge/) . The short quiz tests your knowledge of questions recently asked in a national poll. After completing the quiz, you can compare your score with the general public and learn more about the terms and topics in each question.
>
> Take the Quiz (http://www.pewinternet.org/quiz/cybersecurity-knowledge/)

In an increasingly digital world, an individual's personal data can be as valuable – and as vulnerable – to potential wrongdoers as any other possession. Despite the risk-reducing impact of good cybersecurity habits and the prevalence of cyberattacks on institutions and individuals alike, a Pew Research Center survey finds that many Americans are unclear about some key cybersecurity topics, terms and concepts. A majority of online adults can identify a strong password when they see one and recognize the dangers of using public Wi-Fi. However, many struggle with more technical cybersecurity concepts, such as how to identify true two-factor authentication or determine if a webpage they are using is encrypted.

This survey consisted of 13 questions designed to test Americans' knowledge of a number of cybersecurity issues and terms. Cybersecurity is a complicated and diverse subject, but these questions cover many of the general concepts and basic building blocks that cybersecurity experts stress are important for users to protect themselves online. However, the typical (median) respondent answered only five of these 13 knowledge questions correctly (with a mean of 5.5 correct answers). One-in-five (20%) answered more than eight questions accurately, and just 1% received a "perfect score" by correctly answering all 13 questions.

These are the key findings from an online survey of 1,055 adult internet users living in the United States conducted June 17-27, 2016.

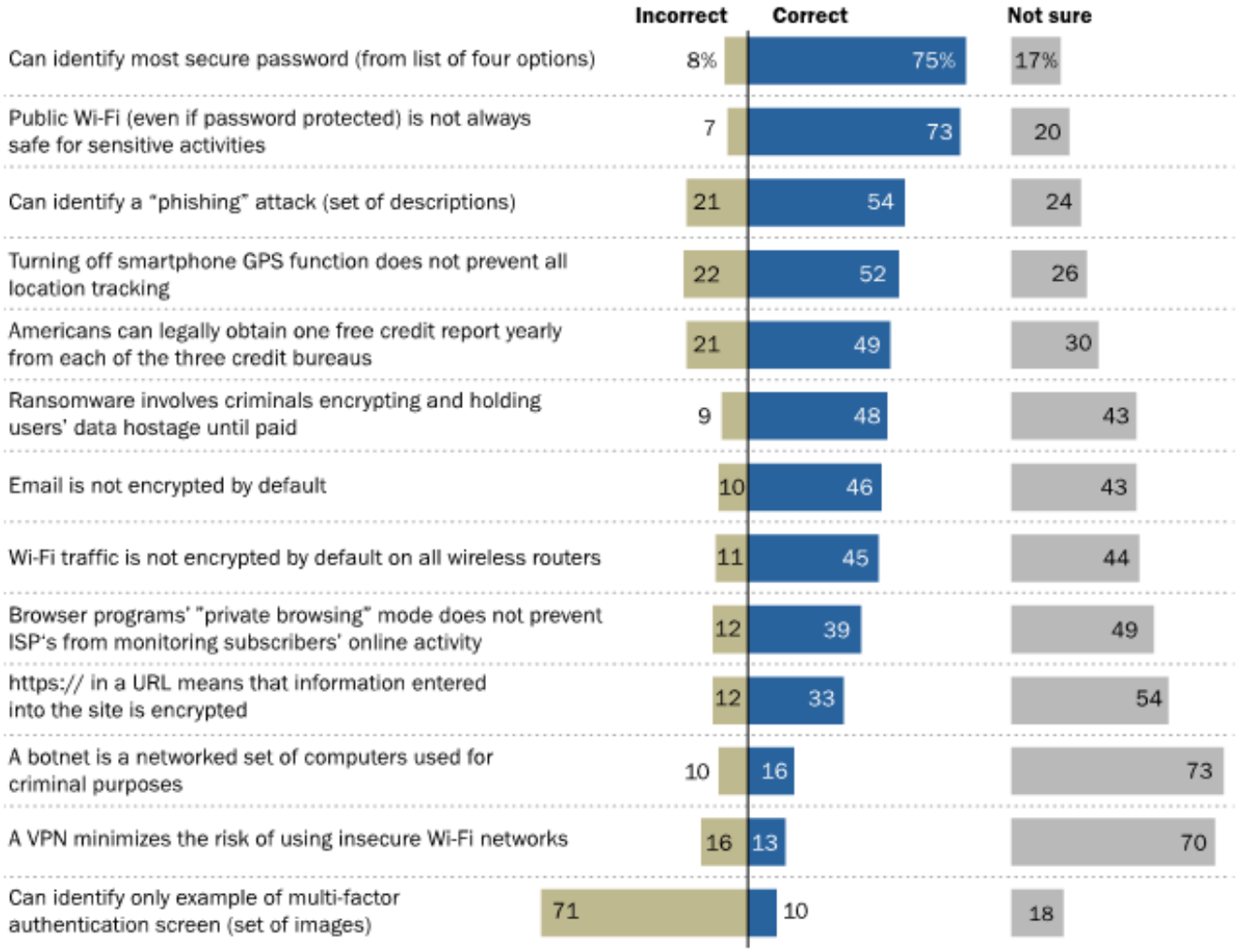
Cybersecurity knowledge varies widely by topic and level of technical detail

Of the 13 questions in the survey, a substantial majority of online adults were able to correctly answer just two of them. First, 75% of online adults can correctly identify the strongest password from a list of four options. The correct password in this case is the password that does not contain words in the dictionary; does contain letters, numbers and symbols; and has a combination of both upper and lower case letters. A similar share (73%) is aware that if a public Wi-Fi network is password protected, it *does not* necessarily mean that it is safe to perform sensitive tasks, such as online banking, using that network.

Meanwhile, around half of internet users are able to correctly answer several other questions in the survey. Some 54% of internet users are able to identify examples of phishing attacks. Similarly, 52% correctly say that turning off the GPS function of a smartphone *does not* prevent all tracking of that device (mobile phones can also be tracked via the cellular towers or Wi-Fi networks to which they are connected).

Many Americans are unsure on a range of cybersecurity topics

% of internet users answering each question ...



Source: Survey conducted June 17-27, 2016.
"What the Public Knows About Cybersecurity"

PEW RESEARCH CENTER

Additionally, 49% of internet users know that Americans are legally entitled to get one free copy of their credit report annually from each of the three major credit bureaus. This issue is not specifically related to any technical aspects of cybersecurity, but cybersecurity experts recommend that anyone who uses the internet for financial or other sensitive transactions regularly check their credit reports to discover evidence of identity theft or other kinds of fraud. A similar share (48%) can correctly define the term "ransomware." This refers to criminals accessing someone's computer, encrypting their personal files and data, and holding that data hostage unless they are paid to decrypt the files.

Americans' practical understanding of email and Wi-Fi encryption is also relatively mixed: 46% of internet users are able to correctly identify that the statement "all email is encrypted by default" is false. Some email services do encrypt users' messages, but this is not a standard feature of all email services. At the same time, 45% correctly identify the statement "all Wi-Fi traffic is encrypted by default on all wireless routers" is also false.

Public knowledge of cybersecurity is lower on some relatively technical issues

Internet users' understanding of the remaining cybersecurity issues measured in the survey is lower – in some cases dramatically so. For instance, 39% of internet users are aware that internet service providers (ISPs) are able to see the sites their customers are visiting while utilizing the "private browsing" mode on their internet browsers. Private browsing mode only prevents the browser itself, and in some cases the user's computer or smartphone, from saving this information – it is still visible to the ISP. And one-third (33%) are aware that the letter "s" in a URL beginning with "https://" indicates that the traffic on that site is encrypted.

Meanwhile, just 16% of online adults are aware that a group of computers that is networked together and used by hackers to steal data is referred to as a "botnet." A similar share (13%) is aware that the risks of using insecure Wi-Fi networks can be minimized by using a virtual private network, or VPN.

Lastly, cybersecurity experts commonly recommend that internet users employ "two-factor" or "multi-factor" authentication on any account where it is available. Two-factor authentication generally requires users to log in to a site using something the user *knows* (such as a traditional password) along with something the user *possesses* (such as a mobile phone or security token), thus providing an additional layer of security in the event that someone's password is hacked or stolen. But when presented with four images of different types of online login screens, just 10% of online adults are able to correctly identify the one – and only one – example in the list of a true multi-factor authentication process. In this case, the correct answer was a picture of a login screen featuring a temporary code sent to a user's phone that will only help them login for a limited period of time. Several of the other answer options illustrated situations in which users were required to perform a secondary action before accessing a page – such as entering a captcha, or answering a security question. However, none of these other options are examples of two-factor authentication.

A significant share of online adults are simply not sure of the correct answer on a number of cybersecurity knowledge questions

Although the share of online adults who can correctly answer questions about cybersecurity issues varies from topic to topic, in most cases the share providing an actual incorrect answer is relatively small. Rather, many users indicate that they simply are not sure of the correct answer to a large number of the questions in this survey.

At the low end, around one-in-five online adults indicate they are not sure how to identify the most secure password from a list (17%), how to identify multi-factor identification (18%) or whether public Wi-Fi is safe for sensitive activities (20%). At the high end, a substantial majority of internet users are not sure what purpose a VPN serves (70%) or what a botnet does (73%). There are also a number of other questions in this survey where “not sure” responses are markedly more common than incorrect answers. These include the definition of ransomware, whether or not email and Wi-Fi traffic are encrypted by default, whether private browsing mode prevents ISPs from monitoring customer activity and how to identify whether or not a webpage is encrypted. In fact, there is only one question on the survey – how to identify a multi-factor authentication screen – for which a larger share of respondents answer incorrectly than indicate they are not able to answer the question at all.

Those with higher levels of education and younger internet users are more likely to answer cybersecurity questions correctly

Broad differences in cybersecurity knowledge by educational attainment

% of internet users answering each question correctly

	HS or less	Some college	College+	College+ – HS or less diff
Wi-Fi traffic is not encrypted by default on all wireless routers.	30%	46%	64%	+34
https:// in a URL means that information entered into the site is encrypted	22	29	54	+32
Email is not encrypted by default	33	44	65	+32
Ransomware involves criminals encrypting and holding users' data hostage until paid	35	47	66	+31
Turning off smartphone GPS function does not prevent all location tracking	38	58	65	+27
Can identify most secure password (from list of four options)	63	77	88	+25
Americans can legally obtain one free credit report yearly from each of the three credit bureaus	38	52	61	+23
Can identify a "phishing" attack (set of descriptions)	45	54	65	+20
Browser programs' "private browsing" mode does not prevent ISPs from monitoring subscribers' online activity	32	37	51	+19
Public Wi-Fi (even if password protected) is not always safe for sensitive activities	65	75	83	+18
A botnet is a networked set of computers used for criminal purposes	11	14	25	+14
Can identify only example of multi-factor authentication screen (set of images)	5	9	19	+14
A VPN minimizes the risk of using insecure Wi-Fi networks	10	11	21	+11
AVERAGE NUMBER CORRECT OVERALL	4.0	5.5	7.0	+3.0

Note: Some college includes those who attended but did not graduate with four-year degrees as well as those with two-year degrees.
Source: Survey conducted June 17-27, 2016.
"What the Public Knows About Cybersecurity"

PEW RESEARCH CENTER

(http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/pi_2017-03-22_cybersecurity-quiz_0-02/) Internet users' knowledge of cybersecurity varies by several demographic factors. The most consistent differences are related to educational attainment.

Those with college degrees or higher answered an average of 7.0 of the 13 questions in the survey correctly, compared with an average of 5.5 among those who have attended but not graduated from college and an average of just 4.0 for those with high school diplomas or less.

Roughly one-quarter (27%) of those with college degrees answered 10 or more questions correctly, compared with 9% of those who have attended but not graduated from college and just 4% of those with high school diplomas or less.

On all 13 questions in the survey, there is at least an 11 percentage point difference in correct answers between the highest- and lowest-educated groups. And there are four questions with a difference of 30 percentage points or more between the highest- and lowest- educated groups. These include whether or not Wi-Fi traffic is encrypted by default on all wireless routers (a difference of 34 points); what “https://” in a URL refers to (32 points); whether or not all email is encrypted by default (32 points); and the definition of ransomware (31 points).

Modest differences in cybersecurity knowledge by age

% of internet users answering each question correctly

	18-29	30-49	50-64	65+	Youngest – oldest diff
Browser programs' "private browsing" mode does not prevent ISPs from monitoring subscribers' online activity	52%	46%	31%	25%	+27
Turning off smartphone GPS function does not prevent all location tracking	63	54	49	40	+23
Can identify only example of multi-factor authentication screen (set of images)	17	14	6	3	+14
A botnet is a networked set of computers used for criminal purposes	24	19	11	10	+14
Public Wi-Fi (even if password protected) is not always safe for sensitive activities	78	72	75	68	+10
https:// in a URL means that information entered into the site is encrypted	33	43	28	26	+7
Wi-Fi traffic is not encrypted by default on all wireless routers.	45	50	44	39	+6
Can identify most secure password (from list of four options)	78	78	69	73	+5
Email is not encrypted by default	46	49	45	42	+4
Ransomware involves criminals encrypting and holding users' data hostage until paid	49	51	46	46	+3
A VPN minimizes the risk of using insecure Wi-Fi networks	13	18	11	10	+3
Americans can legally obtain one free credit report year from each of the three credit bureaus	48	55	45	46	+2
Can identify a "phishing" attack (set of descriptions)	52	55	54	54	-2
AVERAGE NUMBER CORRECT OVERALL	6.0	6.0	5.0	5.0	+1.0

Source: Survey conducted June 17-27, 2016.
" What the Public Knows About Cybersecurity "

PEW RESEARCH CENTER

(http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/pi_2017-03-22_cybersecurity-quiz_0-03/) Cybersecurity knowledge also varies by respondent age, although these differences are much less dramatic than the differences pertaining to educational attainment. Indeed, on a number of these questions internet users age 65 and older are just as knowledgeable as those ages 18 to 29. For instance, older and younger users are equally likely to be able to identify a phishing attack, identify the most secure password from a list and know how many free credit reports Americans are entitled to by law. However, younger users score higher on certain questions – such as whether "private browsing" mode prevents ISPs from tracking users' online activities (a 27 point difference) or whether turning off the GPS feature on a smartphone disables all tracking of that device (a 23 point difference).

Overall, 18- to 29-year-olds correctly answered a mean of 6.0 out of 13 questions, compared with a mean of 5.0 among those 65 and older.

APPENDIX D.20

STRATEGIC RESOURCE WORKING GROUP

2026

STRATEGIC RESOURCE WORKING GROUP STRATEGIC PLAN

Chair: Chetrice Mosley | Co-Chair: Scott Miller

September 2018
Indiana Executive Council on Cybersecurity

Strategic Resource Working Group Plan

Contents

Committee Members **4**
Introduction **7**
Executive Summary **9**
Research **12**
Deliverable: IECC Program Documentation **15**
General information 15
Implementation Plan 16
Evaluation Methodology 20
Deliverable: IECC Scorecard **22**
General information 22
Implementation Plan 23
Evaluation Methodology 27
Deliverable: IECC Sustainability Recommendation **30**
General information 30
Implementation Plan 31
Evaluation Methodology 34
Supporting Documentation **36**
IECC Cybersecurity Scorecard 37

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Chetrice Mosley	State of Indiana	Cybersecurity Program Director	Chair	IECC Director
Scott Miller	Citizens Energy Group	Manager of Security and Compliance	Co-Chair	Advisory
Noel Lephart	Indiana Office of Technology	Program Manager	Full Time	Advisory
Eric Dietz	Purdue	Professor, CIT	Full Time	Advisory
William Mackey	Indiana State University	Professor	Full Time	Advisory
Rich Banta	Lifeline Data Centers	Partner	Full Time	Advisory
Connie Justice	IUPUI	Professor	Full Time	Advisory
Joe Romero	IU Health	Emergency Manager	As Needed	Advisory
Brad Wheeler	Indiana University	CIO	As Needed	Advisory
Mark Bruhn	Indiana University	Associate VP of Public Safety and Institutional Assurance	Full Time	Advisory
Gerry McCartney	Purdue	CIO	As Needed	Advisory
Ron Bush	Ron Bush Consulting	Consultant	As Needed	Advisory
Ron Bushar	Mandiant	Director	As Needed	Advisory
Joe Cudby	Kinney Group	Vice President	Full Time	Advisory
Stephanie Dingman	Aon PLC	Manager	As Needed	Advisory
Matthew Donahue	LexisNexis Risk Solutions	Director	Full Time	Advisory
Michael Frank	Anderson University	N/A	As Needed	Advisory
Jose Gonzales	La Voz	Vice President	As Needed	Advisory
David Greer	Project Lead The Way, Inc.	N/A	As Needed	Advisory
Mike Langelier	Techpoint	President	As Needed	Advisory
Mark Loepker	INsURE	Director	As Needed	Advisory
John Lohrentz	Munster Police Department/NISSA	N/A	As Needed	Advisory

Thomas MacLellan	Symantec	Government Affairs	As Needed	Advisory
Dan Owen	N/A	Independent Consultant	As Needed	Advisory
Tasha Phelps	Phelco Technologies, Inc.	President	As Needed	Advisory
Chad Pittman	Purdue Research Foundation	N/A	As Needed	Advisory
Diana Williams	Project Brilliant	Director	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - National Governors Association (NGA)
  - National Association of State Chief Information Officers (NASCIO)
  - Purdue Homeland Security Project
  - State-to-State Comparison Research
  - Cybersecurity Prediction Reports
  - Fusions Centers
  - Information Sharing and Analysis Centers (ISAC)
  - Indiana Department of Homeland Security (IDHS)/U.S. Department of Homeland Security (USDHS)
  - Policy
  - Conferences
  - Webinars
  - Best Practices/Examples of other Councils and Boards
  - Feedback from Council members before the hiring of the Cybersecurity Program Director

- **Research Findings**
  - It was imperative to understand all aspects of the cyber ecosystem within state government. This included understanding:
    - Fusions Centers
      - https://www.dhs.gov/annual-fusion-center-assessment-and-gap-mitigation-activities
      - http://www.govtech.com/em/safety/National-Fusion-Center-Model-Is-Emerging.html
      - https://nfcausa.org/
      - https://www.dhs.gov/national-network-fusion-centers-fact-sheet
      - https://nfcausa.org/html/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers.pdf
    - Information Sharing
      - National Strategy for Information Sharing: https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/1763-2012-national-strategy-for-information-sharing-and-safeguarding-nsiss
      - ISAC state to state comparison primary research
      - See Research Executive summary for Cyber Sharing Working Group
    - National Guard – See Pre thru Post Incident Working Group Executive Summary
    - IDHS – See Emergency Services and Exercise Executive Summary
    - Federal Partnerships

- **Working Group Deliverables**
  - IECC Framework Documentation
  - IECC Scorecard

- IECC Sustainability Recommendation

- **Additional Notes**
  - **State and Other Example Websites**
    - Cyber Virginia
    - Michigan Cyber Initiative
    - Missouri Office of Cybersecurity
    - Pennsylvania
    - Washington Cybersecurity Program
    - Wisconsin Cybersecurity
    - Multistate Information Sharing and Analysis Center (MS-ISAC)

- **References**
  - Article: Presidential Cybersecurity E.O. - http://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-trump-executive-order-on-cybersecurity-just-an-opening-act.html
  - NGA Meet the Threat - https://www.nga.org/cms/meet-the-threat
  - National Association of State Chief Information Officers (NASCIO) - https://www.nascio.org/
  - PPD 41 – U.S. Cyber Incident Coordination: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
  - U.S. Computer Emergency Readiness Team (US-CERT): https://www.us-cert.gov/
  - Report: State of the States on Cybersecurity (Pell Center)
  - Memo on State Cybersecurity Governance Bodies
  - Memo on State Cybersecurity Response Plans
  - Michigan Cyber Disruption Response Plan
  - NIST Computer Security Incident Handling Guide
  - NASCIO Cyber Disruption Response Planning Guide
  - Building a Cybersecurity Workforce Pipeline

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Crit-Ex 2016
    b. Established Governor Council on Cybersecurity – March 2016
    c. Continued Governor Council on Cybersecurity – January 2017

2. **What (or who) are the most significant cyber vulnerabilities in your area**?
    a. Critical infrastructure, businesses, and individuals

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. A comprehensive, collaborative strategic state-wide cybersecurity approach that will address:
        - Establish an effective governing structure and strategic direction;
        - Formalize strategic cybersecurity partnerships across the public and private sectors.
        - Strengthen best practices to protect information technology infrastructure;
        - Build and maintain robust statewide cyber incident response capabilities;
        - Establish processes, technology, and facilities to improve cybersecurity statewide;
        - Leverage business and economic opportunities related to information, critical infrastructure, and network security; and
        - Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Regulations vary by industry and sector.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Other State Models such as:
        - Cyber Virginia
        - Michigan Cyber Initiative
        - Missouri Office of Cybersecurity
        - Pennsylvania
        - Washington Cybersecurity Program
        - Wisconsin Cybersecurity
        - Multistate Information Sharing and Analysis Center (MS-ISAC)

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. National Governors Association
    b. National Association of State Chief Information Officers (NASCIO)
    c. Purdue Homeland Security Project – in progress
    d. State-to-State Comparison Research – ongoing

e. Cybersecurity Prediction Reports
f. Fusions Centers
g. Information Sharing and Analysis Centers (ISACs)
h. Indiana Department of Homeland Security/United States Department of Homeland Security (IDHS/USDHS)
i. Policy
j. Conferences
k. Webinars
l. Best Practices/Examples of other Councils and Boards
m. Feedback from Council members prior to the hiring of the Cybersecurity Program Director

7. What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?

a. See question 5 and 6.

8. What does success look like for your area in one year, three years, and five years?

a. Developing a sustainability model with appropriate resources that will continue to implement and demonstrate measurable improvement in the state's cybersecurity posture will be vital to the Council's continued success. The model will ensure that the Council continues to develop, maintain, and execute the implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which will be completed within an established timeframe over the next one, three, and five years.

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

a. An overall communication plan to increase cybersecurity awareness, programs, training, and education is needed.

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. N/A

11. What do we need to do to attract cyber companies to Indiana?

a. The State's emphasis on the importance of cybersecurity will attract companies to Indiana.

12. What are your communication protocols in a cyber emergency?

a. N/A

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. See sector specific questionnaire.

Deliverable: IECC Program Documentation

Deliverable: IECC Program Documentation

General information

1. **What is the deliverable?**
   a. IECC Program Documentation

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns.**
   ☒ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Documentation of the creation, implementation, and evaluation of the IECC, including the project plan, framework, governance, tools used, and lessons learned.

6. **What metric or measurement will be used to define success?**
   a. Completion and inclusion of the IECC Program Documentation in the final plan

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. IECC, Governor's office, federal and state partners

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All, as needed

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None

12. **Who should be main lead of this deliverable?**
    a. IECC Director

13. **What are the expected challenges to completing this deliverable?**
    a. None.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Determine what the Framework Document will contain	Program Director, Program Manager	100%	February 2018	
Develop draft Table of Contents	Program Manager	100%	February 2018	
Review draft TOC	Program Director, Program Manager	100%	February 2018	
Develop list of subtopics	Program Director, Program Manager	100%	March – April 2018	
Begin documenting topics and subtopics	Program Manager	100%	March 2018	
Determine document design	Program Director, Program Manager	100%	May-July 2018	
Complete Draft	Program Manager	100%	July 2018	
Final Draft approval	Program Director	100%	July 2018	
Strategic Resource WG approval process	Program Manager	100%	August 2018	
Complete documentation and Final Review	Program Director	100%	August 2018	
Integrate document into final report	Program Director, Program Manager	100%	September 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Providing supporting documentation of how the Council was planned, established, and governed. Sharing a repeatable framework for other organizations and states to leverage.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This framework documentation provides support for the Council's work, and will help support the organization of future Council efforts.

19. What is the risk or cost of not completing this deliverable?

a. The organization and processes used with the Council will be lost and the future movement of the IECC support organization will have less direction and strategy. Knowledge sharing with other states and agencies will not occur.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion of the documentation July 2018 and Strategic Resource Working Group approval. The final Governor's proposal in late September 2018.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No
b. **If Yes, please list states/jurisdictions**
   i. N/A

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No
b. **If Yes, please list states/jurisdictions**
   i. N/A. Because there are no other states doing work like the IECC.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Resource constraints, competing priorities, and a short timeframe.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Cybersecurity Program Director

27. Can this deliverable be used by other sectors?

a. No
b. **If Yes, please list sectors**
    i. It can be used by other states

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. IECC

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes; it will be the Part 1 of the final cybersecurity strategic plan provided to the Governor September 2018

30. What are other public relations and/or marketing considerations to be noted?

a. Further detailed information can be shared with internal management and those who request it, such as the National Governors Association (NGA), and other states.

Evaluation Methodology

Objective 1: IECC will develop program/framework documentation by September 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: IECC Scorecard

Deliverable: IECC Scorecard

General information

1. **What is the deliverable?**
   a. IECC Scorecard

2. **What is the status of this deliverable?**
   a. In-progress; 75% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☒ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☒ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. The goal of the scorecard is two-fold. It will provide a baseline as well as a measurement of the effectiveness of the IECC deliverables as well as a more detailed cybersecurity self-assessment.

6. **What metric or measurement will be used to define success?**
   a. A sentinel sampling of all sectors completing the scorecard and self-assessment.

7. **What year will the deliverable be completed?**
   a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Small and medium sector companies and local government.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Federal and private assessments.

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All, as needed.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IECC partners with Purdue University

12. **Who should be main lead of this deliverable?**
    a. IECC Director with Purdue University

13. **What are the expected challenges to completing this deliverable?**
    a. Scope and participation of the scorecard.

Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Find an IECC partner to assist with developing the scorecard	Cybersecurity Program Director	100%	November 2017	Chose Purdue University
Conduct research of scorecards and assessments	Cybersecurity Program Director and Purdue	100%	January – April 2018	
Draft scorecard	Purdue	100%	March/April 2018	
Review Scorecard	Strategic Resources Working Group	100%	April 2018	
Review Scorecard	IECC	100%	April 2018	
Develop implementation plan	Cybersecurity Program Director and Ivy Tech Resource	100%	May 2018	
Identify sentinel pilot group	All critical infrastructure chairs as well as local government, business, and education sectors	100%	May-June 2018	
Pilot Group complete scorecard	Pilot Group	100%	June - September 2018	
Take survey on product	Cybersecurity Program Director and Purdue	0	October 2018	
Develop implementation plan for mass public	Cybersecurity Program Director and Ivy Tech Resource	0	December 2018	
Pilot Group retake scorecard	Pilot Group	0	March 2019	
Execute implementation plan for mass public	Cybersecurity Program Director	0	2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes
b. If Yes, please complete the following

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1 FTE	N/A	Cybersecurity and business	State of Indiana	IECC Partner	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Measurement of the success of IECC efforts and deliverables and more importantly provide the public a tool (specifically small/medium size businesses and local governments) to start to identify their current cybersecurity posture. Additionally, after making improvements, this gives immediate feedback as to whether the improvement was made.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. This scorecard is meant to assess current-state and address the problem areas most appropriate to the organization surveyed. By doing this at a business level and in a way that can be provided to executive leadership of a company, the scorecard could assist in prioritizing and providing a form of measurement to reducing cybersecurity risk or impact.

19. What is the risk or cost of not completing this deliverable?

a. The state and the IECC will not have a mechanism of measuring progress of Indiana's cybersecurity posture.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion of the scorecard is an output success. Having 90 percent of all sentinel sample complete the scorecard.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. More than 30 states have a cyber council but have not provided a user-friendly scorecard that can be used by the organization, as well as a measurement for the effectiveness of the tools created by the Council.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Short time frame and engaging each sector.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. It was presented to the full Council in April 2018 for input and discussion.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
   i. All

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. IECC, Government, businesses, associations, sector partners

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. No other like this.

Evaluation Methodology

Objective 1: IECC, along with Purdue University, will develop Indiana's first Cybersecurity Scorecard by May 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC, along with Purdue University, will launch Indiana's Cybersecurity Scorecard Pilot Program with 90 percent of selected organizations by September 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Objective 3: IECC, along with Purdue University, will develop a final report of Indiana's Cybersecurity Scorecard Pilot Program by May 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: IECC Sustainability Recommendation

Deliverable: IECC Sustainability Recommendation

General information

1. **What is the deliverable?**
   a. IECC Sustainably Recommendation

2. **What is the status of this deliverable?**
   a. 100% Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
   ☒ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☒ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. The IECC Sustainability Recommendation will help inform the Governor of the next steps with the IECC.

6. **What metric or measurement will be used to define success?**
   a. Adoption of the recommendation by the Governor, his office, and Council partners.

7. **What year will the deliverable be completed?**
   a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Governor and IECC

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All, as needed

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. N/A

12. **Who should be main lead of this deliverable?**
    a. IECC Director

13. **What are the expected challenges to completing this deliverable?**
    a. None

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Research other state approaches	Cybersecurity Program Director and IECC fellow	100%	August 2018	
Draft section to final report	Cybersecurity Program Director and IECC fellow	100%	July 2018	
Review	IECC Core Leadership	100%	September 2018	
Submit with final plan as a memo	Cybersecurity Program Director and IECC	100%	September 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
N/A						

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Positioning the IECC for its continued success in implementing the overall statewide strategy for cybersecurity.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. A sustainability plan will help the State of Indiana and partners to most efficiently continue to provide businesses and governments tools to continue lowering their cybersecurity risks.

19. What is the risk or cost of not completing this deliverable?

a. Efforts of the IECC may slow down or become abandoned.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion of recommendation that provides a comprehensive review of what others have done and a variety of courses of actions Indiana can take.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. Yes

b. **If Yes, please list states/jurisdictions**

   i. There are many models to evaluate over the next several months to consider and explain in the report.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
   i. This will be determined in the research, but more than likely.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Resource constraints and short timeframe.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. N/A

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. None

27. Can this deliverable be used by other sectors?

a. No

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. IECC, Governor's Office, general public

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. A public relations plan will be implemented highlighting the efforts of the IECC and report, which include the sustainability courses of actions.

Evaluation Methodology

Objective 1: IECC will develop a sustainability recommendation for the Council by September 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- IECC Cybersecurity Scorecard

Indiana Executive Council on Cybersecurity (IECC)

Cybersecurity Scorecard

April 2018

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Welcome to the State of Indiana's Cybersecurity Scorecard in partnership with Purdue University!

This Scorecard should take you approximately 10-15 minutes to complete.

For your convenience, this Scorecard is a fillable PDF, can be saved with your answers, and will automatically calculate your score.

For your reference there is a Glossary of Terms on the last page with definitions for technical terms highlighted in blue lettering.

If you have any questions on this Scorecard, please email the Cybersecurity Program Director Chetrice Mosley at mosleyclm@iot.in.gov.

Name of Organization

_____

Your E-mail Address

_____

How many employees are there in your organization (full and part time)?

_____

How many employees have information technology related duties?

_____

How many employees have cybersecurity related duties?

_____

Does your organization outsource your information technology needs?

- Yes
- No

Does your organization outsource your cybersecurity needs?

- Yes
- No

Question 1

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our organization values cybersecurity.						

Question 2

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.)						

Question 3

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)						

Question 4

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our business/organization model influences the way we approach cybersecurity.	○	○	○	○	○	○

Question 5

	I Don’t Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.	○	○	○	○	○	○

Question 6

	I Don’t Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We are familiar with the cybersecurity threats or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees.	○	○	○	○	○	○

Question 7

	I Don’t Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls.						

Question 8

	I Don’t Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have **system checks** in place to make sure that our data is not compromised or changed.						

Question 9

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our data is available to employees or clients when needed. (If our government or commerce site was unavailable to customers or employees, we would know what to do).						

Question 10

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.	○	○	○	○	○	○

Question 11

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our cybersecurity technology (such as **antivirus**, wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data.	○	○	○	○	○	○

Question 12

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have a process in place to address a **cyberthreat**.	○	○	○	○	○	○

Question 13

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have a cyber emergency response plan in place to address a **cyberattack** on our organization.	○	○	○	○	○	○

Question 14

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
If we were impacted by a cyber emergency (e.g. **ransomware**), we know how our organization would recover our data and/or operational systems.	○	○	○	○	○	○

Question 15

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
After a **cyberthreat** or emergency, our organization will make changes to people, process, technology, etc. to improve our security.	○	○	○	○	○	○

Question 16

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our executive leadership receives periodic status, physical, and cybersecurity updates.						

Question 17

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.						

Question 18

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We provide our employees cybersecurity awareness and/or training.						

Question 19

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We protect our business and customer information so that only the employees that need to see it, can.						

Question 20

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We would know if our cybersecurity technology detected a **cyberthreat**.						

Question 21

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.						

Question 22

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software	○	○	○	○	○	○

To find your score, please add the numbers associated with the responses for questions 1 through 22. For example, selecting "Almost Every Time (4)" has a numberical value of 4.

Your score is 0_____

Refer to the chart below to determine where you fall on the scale.

Grade	Exemplary	Accomplished	Developing	Beginning	Undeveloped
Minimum with color code	88	66	44	22	0
Range	110-88	87-66	65-44	43-22	21-0
Spread	22	21	21	21	21

Glossary of Terms

System checks- procedures, equipment, and/or periodic inspection to maintain security
Antivirus- i.e. McAfee, Norton, or Windows Defender
Cyberthreat- the possibility of a malicious attempt to damage or disrupt a computer network or system. For example, social engineered trojans, unpatched software (such as Java, Adobe Reader, Flash), and/or phishing
Cyberattack- an attack initiated from one or more computers against a website, computer system or a networked enterprise of several computers that compromises the confidentiality, integrity or availability of any computer(s) or stored information
Ransomware- a type of malware that prevents users from using their computer and displays messages requiring users to pay a ransom usually through an online payment in order to regain access to his/her computer, information, and/or system.

APPENDIX E

INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY MEMBERSHIP & LEADERSHIP LIST

Indiana Executive Council on Cybersecurity -
Membership as of Last Official IECC Vote on January 2018

Council Voting/Non-Voting Members										
Name - Primary	**Sector**	**Organization**	**Title**	**Email**	**Designee 1**	**Title**	**Email**	**Designee 2**	**Title**	**Email**
John Hammond	State of Indiana	Governor's Office	Senior Operations Director	jhammond2@gov.in.gov	Micah Vincent	OMB Director	mvincent@gov.in.gov			
Bryan Langley	State of Indiana	Indiana Department of Homeland Security	Executive Director	blangley@dhs.in.gov	Jordan Bolden	Chief of Staff	JoBolden@dhs.IN.gov			
Dewand Neely	State of Indiana	Indiana Office of Technology	CIO	dneely@iot.in.gov	Bryan Sacks	CISO	tstahl@iot.in.gov			
Douglas Carter	State of Indiana	Indiana State Police	Superintendent	dcarter@isp.in.gov	Larry Turner	Lt. Col, Office of Superintendent	LTurner@isp.IN.gov	Chuck Cohen	Commander, Intelligence and Investigative Technologies	ccohen@isp.in.gov
MG Courtney Carr	State of Indiana	Indiana National Guard	Adjutant General	courtney.p.carr.mil@mail.mil	Tim Winslow	COL USARMY NG INARNG	timothy.j.winslow.mil@mail.mil	Col. Jeffrey Hackett	INNG Cyber Operations	jeffrey.s.hackett.mil@mail.mil
Connie Lawson	State of Indiana	Secretary of State	Secretary of State	cwlawson@sos.in.gov	Brandon Clifton	Deputy Chief of Staff	bclifton@sos.in.gov			
Jim Huston	State of Indiana	Indiana Utility Regulatory Commission	Chair	JHuston1@urc.in.gov	Sarah Freeman	Commissioner	sfreeman@urc.in.gov			
Teresa Lubbers	State of Indiana	Indiana Commission for Higher Education	Commissioner	tlubbers@che.in.gov	Michael Hawryluk	Chief Technolgoy Officer	MHawryluk@che.in.gov			
Adam Krupp	State of Indiana	Indiana Department of Revenue	Commissioner	AKrupp1@dor.IN.gov	Tony Chu	CISO	TChu@dor.IN.gov			
Jim Schellinger	State of Indiana	Indiana Economic Development Corporation	Secretary of Commerce	JSchellinger@iedc.IN.gov	David Roberts	VP, Chief Innovation Officer	DRoberts2@iedc.IN.gov	Mark Wasky	Policy Director and Counsel, Policy	MWasky@iedc.IN.gov
Brad Wheeler	State of Indiana	Indiana University	CIO	bwheeler@iu.edu	Mark Bruhn	Associate VP of Public Safety and Institutional Assurance	mbruhn@iu.edu			
Curtis Hill	State of Indiana	Attorney General	Attorney General	JeanMarie.Leisher@atg.in.gov	Douglas Swetnam	Section Chief of Data Privacy and Identity Theft Unit	douglas.swetnam@atg.in.gov			
Gerry McCartney	State of Indiana	Purdue University	CIO	mccart@purdue.edu	Greg Hedrick	CISO	hedrick@purdue.edu	Rob Stanfield	Director, Identity Access Management	rob@purdue.edu
Tracy Barnes	State of Indiana	Lt. Governor's Office - CTASC Representative	Chief of Staff	TrBarnes@lg.IN.gov	Ryan Heater	Policy Director	rheater@lg.in.gov	Rebecca Kasper	Special counselor	RKasper@lg.IN.gov
Fred Payne	State of Indiana	Indiana Department of Workforce Development	Commissioner	Fpayne@dwd.in.gov	Steve Elliot	Executive Director	SElliott1@dwd.in.gov			
Danielle Chrysler	State of Indiana	Indiana Office of Defense Development	Director	DChrysler@iodd.IN.gov	Ryan Metzing	Ice Miller	Ryan.Metzing@icemiller.com			
Stephanie Yager	Local Government	Indiana Association of County Commissioners	Executive Director	stephanie@indianacountycommissioners	Mike Yoder	President, Elkhart County	mikeyoder@maplenet.net			
Rhonda Cook	Local Government	Accelerate Indiana Municipalities (AIM)	Executive Director	rcook@aimindiana.org	Matthew Greller	Executive Director & CEO	mgreller@aimindiana.org			
Mark A. Lantzy	Healthcare	IU Health	CIO	mlantzy@IUHealth.org	Mitchell Parker	CISO	mparker17@IUHealth.org			
Joni K. Hart	Communications	Indiana Cable Telecommunications Association	Executive Director	jhart@broadbandig.org	Dan Solero	VP, ATT	dsolero@att.com			
Owen LaChat	Financial Services	MutualBank	Information Security Officer	Owen.LaChat@bankwithmutual.com	Sharon Ferguson	Information Security Officer and CI	sharon.ferguson@bankwithmutual.com			
Stephen A. Key	Public Interest - Media	Hoosier State Press Association	Executive Director	skey@hspa.com	Robert Dittmer	REDCOM Public Relations Consulting, Principal	bob@redcom.biz			
Ronald W. Pelletier	Cybersecurity/IS	Ponderance	Founding Partner	ron.pelletier@pondurance.com	Landon Lewis	Director	landon.lewis@pondurance.com	Dennis Porter	COO	dennis.porter@pondurance.com
John Lucas	Water /Wastewater	Citizens	Vice President, IT	jlucas@CitizensEnergyGroup.com	Jon F. Weirick	Fort Wayne Utilities, Senior Program Manager	Jon.Weirick@cityoffortwayne.org			
Mark T. Maassel	Energy	Indiana Energy Association	President	mmaassel@indianaenergy.org	Robert I. Richhart	Hoosier Energy, Vice President, Management Services	richhart@HEPN.com	Walter Grudzinski	Vectren Corporation, Director, Information Security and Business Continuity	wgrudzinski@Vectren.com
David Ehinger	Defense Industrial Base	Rolls Royce	Business Manager for IT Security	David.P.Ehinger@Rolls-Royce.com	Brad Swearington	Rolls Royce	Brad.Swearingen@Rolls-Royce.com	Mary Kate Frazier	Rolls Royce	MaryKate.Frazier@Liberty.Rolls-Royce.com
John Davidson	FBI	FBI - Indianapolis Field Office	Supervisory Special Agent	jrdavidson@fbi.gov	Michael Alford	Supervisory Special Agent	michael.alford@ic.fbi.gov			
Paul Dvorak	US DHS	Secret Service	Special Agent in Charge	paul.dvorak@usss.dhs.gov						
Tony Enriquez	US DHS	US DHS	Cyber Security Advisor	antonio.enriquez@hq.dhs.gov						

Indiana Executive Council on Cybersecurity -
Membership as of Last Official IECC Vote on January 2018

Advisory Members

Government Advisory Members

Name	Organization	Title
Chris Judge	US DHS	PSA
Kathy Dayhoff-Dwyer	Indiana Department of Homeland Security	District Coordinator Liaison
Brian Rockensuess	Indiana Department of Environmental Management	Chief of Staff
Tom Vanderpool	Indiana Department of Transportation	Director, Emergency Planning and Response, Highway Management
Chris Collins	Infragard	President's Proxy
Brian O'Hara	FBI/Infragard	President of Infragard
David Woodward	Indiana Department of Education	Safety Academy Director
Nick Sturgeon	Pondurance	Security Operations Center Director
Nick Goodwin	Indiana Department of Workforce Development	Program Policy Director
LT Dave Skalon	Indiana National Guard	INNG Cyber Mission
MAJ Jason Brady	Indiana National Guard	INNH DOMS
James Gordon	Indiana National Guard	INNG
Gary Deckord	Atterbury-Muscatatuck Center	Chief, Technology Division
Chris Carter	Indiana State Police	ISP Trooper, Criminal Investigation
Ryan Myers	Indiana State Police	ISP Trooper, Criminal Investigation
Nicole Needman	Indiana Office of Technology	Security Awareness Manager
Graig Lubsen	Indiana Office of Technology	Director of Communications
Thomas Vessley	Secretary of State	Director of IT
Valarie Warycha	Secretary of State	Communcaitons Director
Jerry Bonnet	Secretary of State	General Council
Shane Springer	DWD	Policy Director
Patrick Glover	Secretary of State	Assistant Director of IT
Kelly B. Wittman	Indiana Department of Education	Chief Academic Officer
Dr. John Keller	Indiana Department of Education	Chief Information Officer, Information Technology
Mr. David B. Tygart	National Guard	J36, INNG
Chris Mertens	Hamilton County	IT
Rob Nolley	City of Shelbyville	Council President
Mary Ferndon	City of Columbus	Director
James Haley	City of Fort Wayne	IT
Kathleen M. (IP) Guider	FBI	Outreach Coordinator
Ted Cotterill	Management Performance Hub	Chief Privacy Officer and General Counsel
Amy L. Beard	Indiana Department of Insurance	General Counsel
James F. Ehrenberg	IOT	General Counsel
Brad King	Indiana Election Commission	Election Division Co-Director
Angie Nussmeyer	Indiana Election Commission	Election Division Co-Director
Laura Herzog	Hendricks County	Elections Supervisor
CPT Johnathan Rupel	INNG Cyber Operations	Indiana National Guard
Joseph Meluch	Indiana Department of Homeland Security	EOC Manager

Indiana Executive Council on Cybersecurity -
Membership as of Last Official IECC Vote on January 2018

Erin Rowe	Indiana Department of Homeland Security	Recovery and Response Director
Britt Luke	Office of Publice Access Councilor	Publice Access Councilor
Ashley Schenck	Management Performance Hub	Analytics
Cliff McCullough	Family and Social Services Administration	Deputy/Asst IT Director, Privacy & Security
Lora Walker	Management Performance Hub	Project Manager, Operations
Ken Sauer	Commission for Higher Education	Sr. Assoc. Commissioner and Chief Academic Officer, Academic Affairs
David Murtaugh	Criminal Justice Institute	Executive Director
John Clawson	BMV	Director Of Fraud and Security Enforcement, Fraud and Security Enforcement
Travis Goodwin	Indiana Department of Environmental Management	Senior Environmental Manager, Office of Water Quality/Drinking Water Branch
Peter Lacy	BMV	Commissioner
Brad Stone	Department of Financial Institutions	Director of Information Technology
Tom Fite	Department of Financial Institutions	Director
Kevin Stouder	Department of Financial Institutions	IT Examiner
Tad Stahl	IOT	IN-ISAC Manager
Private and Academic Sector Advisory Members		
Name	**Organization**	**Title**
Cliff Campbell	Campbell Consulting LLC	President
Scott Bowers	Indiana Electric Coops	Vice President of Government Relations
Daniel J. Solero	AT&T	Executive Director, Tech Security
Douglas Rapp	Cyber Leadership Alliance	President
William Mackey	Indiana State University	Assistant Professor
Valita Fredland	Indiana Health Exchange	Vice President – General Counsel and Privacy Officer
Stephen Reynolds	Ice Miller	Partner
Frank Nevers	Eskenazi Health	Information Security Officer
Jamie Lee	Wabash National Corporation	VP and CIO
Paul Mcaninch	IU Health	Director Information Security & Compliance
Leon Ravenna	KAR Auction Services	CISO
Carlos Garcia	Indiana University-Purdue University Indianapolis (IUPUI)	Director, Emergency Management & Continuity
Martin Wessler	Wessler Engineering	CEO
Joseph Romero	IU Health	Emergency Preparedness Program Manager
Scott Miller	Citizens Energy Group	Cyber Security Manager
Duane Gilles	Evansville Water and Sewer Utility	Water Distribution Manager
Steve Berube	Citizens Energy Group	Manager, Water System Control and Planning
David R. Day	IU Health	Manager Governance, Risk, and Compliance
Jacob Butler	Parkview Health	Information Security and Compliance Specialist
Carolyn Wright	IMPA	Vice President of Government Relations
Kim Milford	Indiana University	Lead REN-ISAC
Omer Clifton Tooley	National Center for Complex Operations, Inc.	CEO
Paul Baltzell	CIO	Indiana Economic Development Corporation

Indiana Executive Council on Cybersecurity -
Membership as of Last Official IECC Vote on January 2018

JJ Thompson	Rook Security	CEO
Kyle Werner	Crane	Director of Innovation
Jaimie Foreman	City of Carmel Water, INWARN	Supervisor
Doug Brock	Indiana American Water	Vice President, Operations
J. Kurt Aikman	MISO ENERGY	Manager, Physical Security & Safety
Greg Ellis	Indiana Chamber of Commerce	Vice President, Environmental & Energy Policy
Julie Vincent	IUPUI	Lecturer of Public Relations
Stan Partlow	American Electric Power (AEP)	VP & Chief Security Officer
Kathleen Johnston	Media Freelancer	Media Freelancer
Scott Berry	Indiana Municipal Power Agency	Senior Engineer, Generation, & Compliance
George Lyle	Purdue University	IT Security Risk Analyst I
Andy VanZee	Indiana Hospital Associaiton	Vice President
Brian W. Vitale	Notre Dame Federal Credit Union	Chief Risk and Compliance Officer/Chief Auditor/ Bank Secrecy Act Officer
Micael Servas	Bank with Mutual	SR. INFORMATION SECURITY ANALYST
Tim Berry	Crowe Horwath	Director
Bill Wilson	Indiana Sherriffs' Association	Coordinator
Pam Schmelz	Ivy Tech	Associate Professor/Department Chair/Cybersecurity Chair
Rami Salahieh	Ivy Tech/ NISSA	CSIA Cyber Security Professor/NIISSA Cyber Security Group
Matthew Etchison	Ivy Tech	Vice President of IT/School of Computing and Infomatics
J. Eric Dietz	Purdue University	Director, Purdue Homeland Security Institute and Professor, Computer and Information Technology
Beth Dlug	Allen County Election Board	Director of Elections
Jay Phelps	Bartholomew County	Clerk of the Circuit and Superior Court
Mark Swearingen	Hall, Render, Killian, Heath & Lyman, P.C.	Attorney
Chad Pollitt	Native Advertising Institute	VP of Audience
Barry Ritter	Indiana Statewide 911 Board	Executive Director
Mitch Parker	IU Health	Executive Director/CISO
William Tucket	Navient	Senior Manager of Network Security
Tyler Waters	Police Technical	Director of Marketing
Jo Angela Woods	Accelerate Indiana Muncipalities	General Councel
Matthew Cloud	Ivy Tech	Project Director – TAACCCT Grant; Systems Office-Workforce Alignment
Benjamin Marrero	Ivy Tech	Department Chair, School of Computing and Informatics
Jan Campbell	Leeuw Oberlies & Campbell, P.C.	Partner
Bill Russell	Cummins, Inc.	CISO
Seth Cooper	Baker Tilly Virchow Krause, LLP,	Manager
Darryl K Togashi	Ivy Tech	Department Chair – Cyber Security (CSIA
Sean Fahey	GCR	Elections and Campaign Finance Director
Jay Bagga	Ball State	Voting System Technical Oversite Program (VSTOP)
John Greene	New Libson Telephone Company	CEO and GM
James E. Goldman	Salesforce	Vice President, Security Governance, Risk Management, & Compliance
Sean Roberts	Code.org	Director of State Government Affairs

Indiana Executive Council on Cybersecurity -
Membership as of Last Official IECC Vote on January 2018

David Greer	Project Lead The Way	Senior Vice President and Chief Program Officer
Benjamin Carter	Indianapolis Public Schools	Director of Career & Technical Education
Geanie Umberger, PhD, MSPH, RPh	Purdue University	Associate Dean for Engagement; Clinical Professor, Department of Leadership, Technology and Innovation and Biotechnology and Regulatory Sciences Center
David Vice	Integrated Public Safety Commission	Executive Director, IPSC
Gary Light	Memorial Hospital and Health Care Center	Vice President, CIO
Anthony Vespa	Vespa Group, LLC	Founder
Alejandro “Alex” Valle	Cititzen's	Senior Legal Counsel
Robert Putnam	Gregory & Appel Insurance	Vice President, Property & Casualty Insurance and Risk Management
Stephanie Dingman	Aon	Senior Vice President
Dan Owen	Independent Consultant	President
Brian McGinnis	Barnes & Thornburg	Partner
Ron Bushar	Mandiant/FireEye	VP/Global Government Services
Lisa Berry Tayman	Cyber Scout	Privacy, Information Governance, and GDPR Professional
Jim Weber	Ratheon	System Engineering Department Manager for Cyber Security and Specialty Engineering
Anthony Ferrante	FTI Consulting	Senior Managing Director and Head of Cybersecurity
Todd Vare	Barnes & Thornburg	Patner
Matthew Donahue	LexisNexis Risk Solutions	Director of Market Planning, Tax and Revenue
Andrew Korty	Indiana University	Acting CISO
Tom Gorup	Rook Security	Director of Security Operations
Nicholas Reuhs	Ice Miller	Partner
Dr. Connie Justice, CISSP, DSc.	IUPUI	Professor
Brandi Fabel	Ivy Tech	Assistant Program Chair Professor
Allen Brown	Midwest Natural Gas	Executive
Bryan Sacks	Indiana Office of Technology	CISO
Mike Langelier	TechPoint	President
Dom Caristi	Ball State	Professor
Stephen G. Scofes	Scofes & Associates Consulting, Inc	Chairman & CEO
Greg Faremouth	Scofes & Associates Consulting, Inc	Partner
Rich Banta	Lifeline Datacenters	Owner
Kevin Mabry	Sentree Systems, Corp	CEO
Dave Sturgeon	Tippecanoe County	Chief Information Officer
Jonathan Barefoot	Ivy Tech	Executive Director of Statewide Safety and Security
Daniel Calarco	Indiana University	Chief of Staff for VP of IT and CIO
Mike Alley	Reslient Strategy	President
Joe Cudby	Kinney Group	VP
Mary Kate Frazier	Rolls Royce	Sr. Security Strategy Officer
Michael W Frank	Anderson University	Director
John Lohrentz	Munster Police Dept/NISSA	Cyber Security Member
Will Dantzler	CLA	Associate
Chad Pittman	Purdue Research Foundation	VP
Chuck McCormick	ESCO Communications	Solutions Engineer

Indiana Executive Council on Cybersecurity -
Membership as of Last Official IECC Vote on January 2018

Diana Williams	Project Brilliant	Director
Von Welch	Indiana University	Director
Tasha Phelps	Phelco	Owner
Mathew Norris	Krieg DeVault LLP / Satelite Association	Counsel
Paul Mitchell	Energy Systems Network	CEO
Jose Gonzalez	La Voz	Vice President
Brad Swearington	Rolls Royce	Director of Engineering – Controls, North America
Emmanuel Ndow	Marion General Hospital	Chief Information Officer
Thomas MacLellan	Symantec	Policy Director
John Knies	CenturyLink	Director & Chief Information Security Officer
Ed Reuter	911 Board	Director of the Board
Richard Braidich	RCR Technology	CISO
Kimberly Metzger	Ice Miller	Partner
Jennifer De Medeiros	The AES Corporation	Infrastructure Security Analyst

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Committee and Working Group Leadership List
Updated July 2018

- Government Service
  - Chair: Superintendent Doug Carter
  - Chair Proxy: Capt. Chuck Cohen
  - Co-Chair: FBI Supervisory Special Agent in Charge John Davidson
- Finance
  - Chair: Owen LaChat
  - Co-Chair: Tom Fite
- Energy
  - Chair: Mark T. Maassel
  - Co-Chair: Robert I. Richhart
- Water and Wastewater
  - Chair: John Lucas
  - Co-Chair: Jon F. Weirick
- Communications
  - Chair: Joni K. Hart
  - Co-Chair: Daniel J. Solero
- Healthcare
  - Chair: Mark A. Lantzy
  - Chair Proxy: Mitchell Parker
  - Co-Chair: Jacob Butler
- Defense Industrial
  - Chair: Director Danielle Chrysler
  - Co-Chair: Kyle Werner
- Elections
  - Chair: Secretary Connie Lawson
  - Co-Chair: Beth Dlug
- Economic Development
  - Chair: Secretary Jim Schellinger
  - Chair Proxy: David Roberts
  - Co-Chair: Ronald W. Pelletier
- Workforce Development
  - Chair: Commissioner Fred Payne
  - Chair Proxy: Jeff Tucker
  - Co-Chair: Dr. John Keller
- Personal Identifiable Information
  - Chair: CIO Dewand Neely
  - Chair Proxy: Ted Cotterill
  - Co-Chair: Valita Fredland

- Public Awareness and Training
    - Chair: Stephen A. Key
    - Co-Chair: Robert Dittmer
- Emergency Services and Exercise
    - Chair: Executive Director Bryan Langley
    - Co-Chair: Carlos Garcia
    - Co-Chair Proxy: Joe Romero
- Cyber Sharing
    - Chair: CIO Dewand Neely
    - Chair Proxy: Tad Stahl
    - Co-Chair: Ronald W. Pelletier
- Policy
    - Chair: Chetrice Mosley
    - Co-Chair: Lt. Governor Chief of Staff Tracy Barnes
- Pre to Post Incident
    - Chair: MG Courtney Carr
    - Chair Proxy: Col. Jeffery Hackett
    - Co-Chair: CIO Dewand Neely
- Legal/Insurance
    - Chair: Attorney General Curtis Hill
    - Chair Proxy: Douglas Swetnam
    - Co-Chair: Stephen Reynolds
- Local Government
    - Chair: Rhonda Cook
    - Co-Chair: Stephanie Yager
- Cyber Summit
    - Chair: Chetrice Mosley
    - Co-Chair: Doug Rapp
- Strategic Resource
    - Chair: Chetrice Mosley
    - Co-Chair: Scott Miller

APPENDIX F

INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY EXECUTIVE ORDER GOALS - DELIVERABLES

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

COMMITTEE AND WORKING GROUP DELIVERABLES BY IECC EXECUTIVE ORDER GOAL

Note: Many of the following deliverables meets more than one IECC goal, but for a high-level overview only the primary goal is shown.

Establish an effective governing structure and strategic direction.

1. Energy Committee – Deliverable: Critical Infrastructure Information
2. Energy Committee – Deliverable: Metrics
3. Policy Working Group – Deliverable: Policy Research Report
4. Cyber Sharing Working Group – Deliverable: Best Practices
5. Strategic Resource Working Group – Deliverable: IECC Program Documentation
6. Strategic Resource Working Group – Deliverable: IECC Scorecard
7. Strategic Resource Working Group – Deliverable: IECC Sustainability Recommendation
8. Water/Wastewater Committee – Deliverable: Training Plan

Formalize strategic cybersecurity partnerships across the public and private sectors.

1. Cyber Sharing Working Group – Deliverable: Secured Information Sharing Program
2. Energy Committee – Deliverable: Coordinate with Others
3. Economic Committee – Deliverable: Implementation Plan for Cybersecurity – Marketing
4. Economic Committee – Deliverable: Cybersecurity SIoT Innovation District
5. Defense Industry Committee – Deliverable: Cyber Market System
6. Elections Committee – Deliverable: Election Cybersecurity Public Education and Awareness
7. Cyber Summit Working Group – Deliverable: Cybertech Midwest
8. Government Services Committee – Deliverable: Indiana Cyber Disruption/Emergency Plan

Strengthen best practices to protect information technology infrastructure.

1. PII Working Group – Deliverable: Indiana PII Guidebook
2. Pre- thru Post- Incident Working Group – Deliverable: Exercise
3. Pre- thru Post- Incident Working Group – Deliverable: Gap Analysis
4. Pre- thru Post- Incident Working Group – Deliverable: Cyber Assessments

5. Economic Committee – Deliverable: Incentive Program
6. Cyber Sharing Working Group – Deliverable: Cyber Sharing Maturity Model
7. Communications Committee – Deliverable: Communications Sector Terminology Glossary
8. Communications Committee – Deliverable: Communications Sector Whitepaper
9. Elections Committee – Deliverable: Election System Physical and Logical Security Controls
10. Elections Committee – Deliverable: Cyber Threat Awareness and Training for County Election Administrators
11. Elections Committee – Deliverable: Indiana Best Practices Manual for the Operation of Election Equipment
12. Elections Committee – Deliverable: Catalog and Summaries of Best Election Cybersecurity Reports and Guides
13. Finance Committee – Deliverable: Cyber Training (Ivy Tech)
14. Healthcare Committee – Deliverable: Vendor Management
15. Local Government Working Group – Deliverable: Local Officials Guidebook
16. Water/Wastewater Committee – Deliverable: Cyber Plan Template
17. Public Awareness and Training Working Group – Deliverable: Statewide Cybersecurity Public Relations Plan
18. Legal and Insurance Working Group – Deliverable: Insurance Guide
19. Legal and Insurance Working Group – Deliverable: Policy Review

Build and maintain robust statewide cyber-incident response capabilities.

1. Energy Committee – Deliverable: Contacts
2. Pre- thru Post- Incident Working Group – Deliverable: Cyber Emergency Response Team (IN-CERT)
3. Communications Committee – Deliverable: Cyber Incident Response Engagement Guidance
4. Elections Committee – Deliverable: Election Day Cybersecurity Emergency Preparedness Plans
5. Elections Committee – Deliverable: Election Day Cybersecurity Tabletop Exercises
6. Elections Committee – Deliverable: Election Day Cybersecurity Monitoring and Rapid Response Technical Support
7. Elections Committee – Deliverable: Election Cybersecurity Incident Response and Communications
8. Healthcare Committee – Deliverable: Long-Term Education
9. Healthcare Committee – Deliverable: Indiana Threat Intelligence Distribution System
10. Water/Wastewater Committee – Deliverable: Cyber Contact
11. Emergency Services and Exercise Working Group – Deliverable: Annex

12. Emergency Services and Exercise Working Group – Deliverable: IDHS Exercise Management
13. Emergency Services and Exercise Working Group – Deliverable: EOC
14. Emergency Services and Exercise Working Group – Deliverable: Toolkit

Establish processes, technology, and facilities to improve cybersecurity statewide.

1. Cyber Sharing Working Group – Deliverable: Inventory of Cyber Sharing Resources
2. Cyber Sharing Working Group – Deliverable: MS-ISAC Member Recruitment
3. Communications Committee – Deliverable: Voluntary Industry Contact List
4. Defense Industry Committee – Deliverable: Cyber Statewide Testbed
5. Elections Committee – Deliverable: Statewide Voter Registration (SVRS) Cybersecurity Enhancements
6. Elections Committee – Deliverable: SVRS Network User Access Control Enhancement
7. Elections Committee – Deliverable: Post-Election Risk Limiting Audit Standards and Pilot Program
8. Finance Committee – Deliverable: Top Security Tips Material
9. Government Services Committee – Deliverable: Indiana's Cybersecurity Hub Website
10. Water/Wastewater Committee – Deliverable: Cyber Risk Model (Plan)
11. Water/Wastewater Committee – Deliverable: Risk Tool

Leverage business and economic opportunities related to information, critical infrastructure, and network security.

1. Defense Industry Committee – Deliverable: Cyber Digital Platform
2. Legal and Insurance Working Group – Deliverable: Cyber Insurance Survey

Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

1. Energy Committee – Deliverable: Training
2. Workforce Development Committee – Deliverable: Generate Interest Plan
3. Workforce Development Committee – Deliverable: Job Demand Tool
4. Workforce Development Committee – Deliverable: K-12 Offering Cybersecurity Content
5. Workforce Development Committee – Deliverable: NICE Framework Standard
6. Workforce Development Committee – Deliverable: Incentivized Cybersecurity Certifications
7. Workforce Development Committee – Deliverable: Program Data Tool