# Indiana
## Cybersecurity Strategic Plan


**October 2021**

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

October 29, 2021

Dear Governor Holcomb:

Since 2018, the Indiana Executive Council on Cybersecurity has not only been successful with its first-of-its-kind strategic approach, but it has stepped up in the last year and a half as we have all experienced not only a different world, but some of the largest cyber attacks recorded in history.

And as millions had to become remote in a matter of days, many of the leaders within the Council provided additional deliverables and resources because businesses and local governments needed it.

These cyber warriors and their efforts on your Council have made Indiana a leading state in the nation. In fact, the Council has completed 78 percent of its 69 identified deliverables, and 77 percent of the 120 objectives identified in the strategic plan we presented to you in 2018 even with the challenges of the pandemic. Moreover, these dedicated members have donated hundreds of hours and millions of dollars of services to the businesses, local governments, and citizens in Indiana - an unprecedented amount of savings from a volunteer government Council or Commission.

Due to the success of the previous plan as well as the more than 250 dedicated subject matter experts, the following *2021 Indiana Cybersecurity Strategic Plan* encompasses not only the breadth of topics, but depth as well. The following plan will provide you the background of how we have created the proven strategic framework that we continue to use today, and the plans of 68 deliverables and 134 objectives we will strive to complete in the coming years.

As we work to implement this plan, the Council asks for your continued leadership in:

- Supporting the development of local government cybersecurity resources and education;
- Encouraging the highest-level of 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;

- Supporting a statewide cybersecurity public relations and awareness campaign;
- Encouraging all of Indiana's workforce ecosystem to follow national standards and develop the cybersecurity pipeline; and
- Supporting the Council as it moves forward, including ensuring its membership matches the needs of the state.

We appreciate the opportunity to work with so many great cyber warriors on the Council. Through these partnerships the State is able to best serve Hoosiers and further move Indiana's cybersecurity efforts to the *Next Level*.

Sincerely,

**Executive Director Stephen Cox**
Indiana Department of Homeland Security

**Chief Information Officer Tracy Barnes**
Indiana Office of Technology

**Adjutant General, Brigadier General Dale Lyles**
Indiana National Guard

**Superintendent Doug Carter**
Indiana State Police

**Cybersecurity Program Director Chetrice L. Mosley-Romero**
State of Indiana

# Indiana Executive Council on Cybersecurity

## 2021 Voting Members

Operations Director Samuel Hyer, Office of Governor Eric J. Holcomb
Director John Roeder, Office of Lt. Governor Suzanne Crouch
Executive Director Stephen Cox, Indiana Department of Homeland Security
Chief Information Officer and Director Tracy Barnes, Indiana Office of Technology
Superintendent Douglas Carter, Indiana State Police
Adjutant General, Brigadier General Dale Lyles, Indiana National Guard
Cybersecurity Program Director Chetrice L. Mosley-Romero, State of Indiana
Secretary of State Holli Sullivan, State of Indiana
Attorney General Todd Rokita, State of Indiana
Chair James Huston, Indiana Utility Regulatory Commission
Commissioner Teresa Lubbers, Indiana Commission for Higher Education
Commissioner Bob Grennes, Indiana Department of Revenue
Secretary of Commerce Brad Chambers, Indiana Economic Development Corporation
Commissioner Fred Payne, Indiana Department of Workforce Development
Retired Major General Clif Tooley, Indiana Economic Development Corporation Defense Development
Chief Information Security Officer, Angie Ritchey
Tim Harmon, Journalist
Partner Ronald W. Pelletier, Pondurance
Information Technology Vice President John Lucas, Citizens Energy Group
President Daniel McGrath, Indiana Energy Association
Executive Director Matthew Greller, Accelerate Indiana Municipalities (AIM)
Executive Director Stephanie Yager, Indiana Association of County Commissioners
Chief Information Security Officer Mitch Parker, Indiana University Health
Assistant Vice President of Cybersecurity Dan Solero, AT&T
Director of Cybersecurity Defense Products Brad Swearingen, Rolls Royce
Chief Information Officer Rob Lowden, Indiana University
Chief Information Officer Ian Hyatt, Purdue University

# 2021 Indiana Cybersecurity Strategic Plan

## Table of Contents



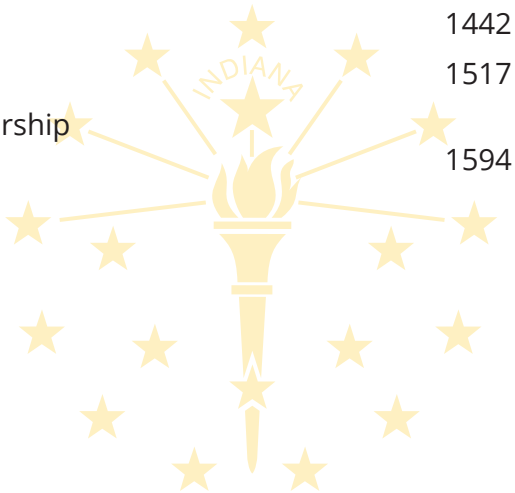
*... continued on next page*

# 2021 Indiana Cybersecurity Strategic Plan

## Table of Contents

## Appendices (continued)






# About This Plan

**Our goals can only be reached through a vehicle of a plan, in which we must fervently believe, and upon which we must vigorously act. There is no other route to success.**

- Pablo Picasso

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, but where the state will go next.

This Indiana cybersecurity strategic plan outlines those directions as simply and as directly as the complexity of the effort allows.

The *2021 Indiana Cybersecurity Strategic 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 summary of the work of the Council.

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 15 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 committee and working group plan is provided in its entirety in the Appendices of this strategic plan.

Part Three highlights the real people and real work since the 2018 plan. The section identifies the dedicated members and leaders of the Council who have dedicated themselves since the beginning, the success of the 2018 plans and more that will be featured in the "The State of Cyber Report", best practices of the Council, and how the Council will continue taking cybersecurity in Indiana to the *Next Level*.


# Part 1
# Strategic Framework of IECC

## Today's Evolving Cyber Threat

A lot has changed since the first Indiana Cybersecurity Strategy was voted on and delivered to Governor Holcomb by the IECC September 2018. But nothing has moved the state of business, workplace culture, and technology more than the months that followed Indiana's pandemic shut down in March 2020. And the reality of how interconnected we all are became even more evident when home became our new workplace and all the cyber risks that followed.

Unfortunately, the new interconnectivity has also made the cyber risks grow exponentially and poses an increased danger to citizens, organizations, and industries, as well as threatens the security and economy of Indiana.

In fact, Cisco's first Hybrid Work Index report found that hybrid workers remain a prime attack vector and that malicious remote access attempts increased 240 percent during the pandemic.

This, of course, is compounded by the fact that the overall leading cause of cybersecurity breaches are still people. According to the Verizon 2021 Data Breach report, 85 percent of breaches were caused by a human element. The 2021 Verizon Data Breach report also found that 61 percent of attacks involved use of unauthorized credentials, and phishing rose to 36 percent (up from 25 percent). And when one phishing exercise — like a malicious email — hits its target, the whole organization is at risk of compromise.

# Indiana's History in Cybersecurity

To understand how the Council came to be, it is important to understand the history of the state's cybersecurity efforts.

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 was 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.

After this inaugural cyber exercise, it became even 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. While the Indiana Executive Council on Cybersecurity (IECC or Council) was established in 2016, it did not become operational until Governor Eric J. Holcomb took office, with a renewed focus and priority through his decision to extend Executive Order 17-11 (See Appendix A).

Per Executive Order 17-11, the Council will:

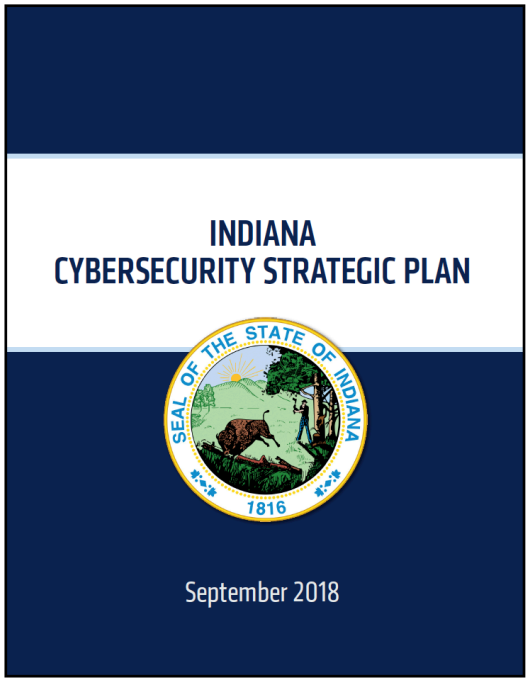
- Develop, maintain, and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe.
- Establish and maintain a strategic framework 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 Security Council, and report to the Homeland Security Advisor within the Office of the Governor.

Given the challenges and complexities surrounding the Executive Order's aims, it became imperative in 2017 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. The purpose of this unique role was for information to be shared across agencies 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.

Using a comprehensive approach to its strategy as described in the next section, the Council delivered an actionable strategic plan to Governor Holcomb on Sept. 21, 2018. The *2018 Indiana Cybersecurity Strategic Plan* encompassed not only the breadth of topics but the depth as well. While the more than 2,000-page 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 their sector within the state.

The *2018 Cybersecurity Strategic Plan* can be found at www.in.gov/cybersecurity.



# Developing the Council and the Strategy

To build and best utilize the cross-sector body of subject-matter experts to effectively understand Indiana's cyber risk profile, identify priorities and develop resources that those who needed it most could access them, and leverage the convened talent from all sectors to stay on the forefront of the cyber risk environment, the Cybersecurity Program Director worked with leadership to establish a strategic framework to be successful in Indiana's cybersecurity initiatives.

## Composition of the Council

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.

Since 2017, the Council has reviewed its Charter, members, and priorities during its quarterly meetings. For example, its Charter, found in Appendix B, is reviewed, and voted on every year, which 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 originally organized into 20 committees and working groups composed of the more than 250 respective members who are experts in their relative fields. As more complex, mature deliverables were crossing over into other committees and working groups it was important to leadership to remain efficient and respectful of those who served on the Council. In January 2020, the Council moved its organization into 15 committees and working groups (See Figure 1). Maintaining this cybersecurity ecosystem while remaining flexible to the work the Council was doing was the only way to achieve maximum results in a relatively short amount of time with the depth of knowledge needed to make informed operational decisions. This became even more important as the world changed in the following months.

Each committee/working group has a smaller charter that 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 were chaired by a Voting Member of the Council to ensure that all plans were aligned with the goals of the entire Council.

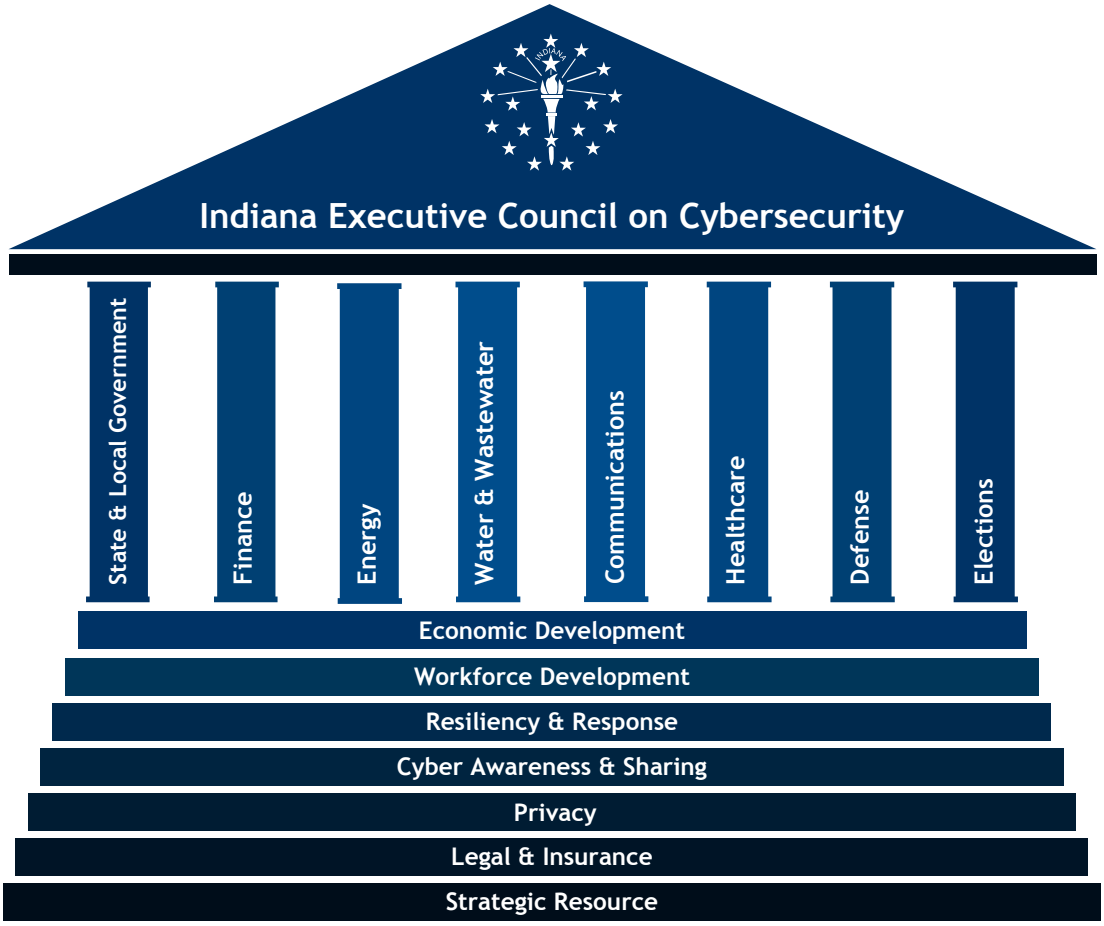
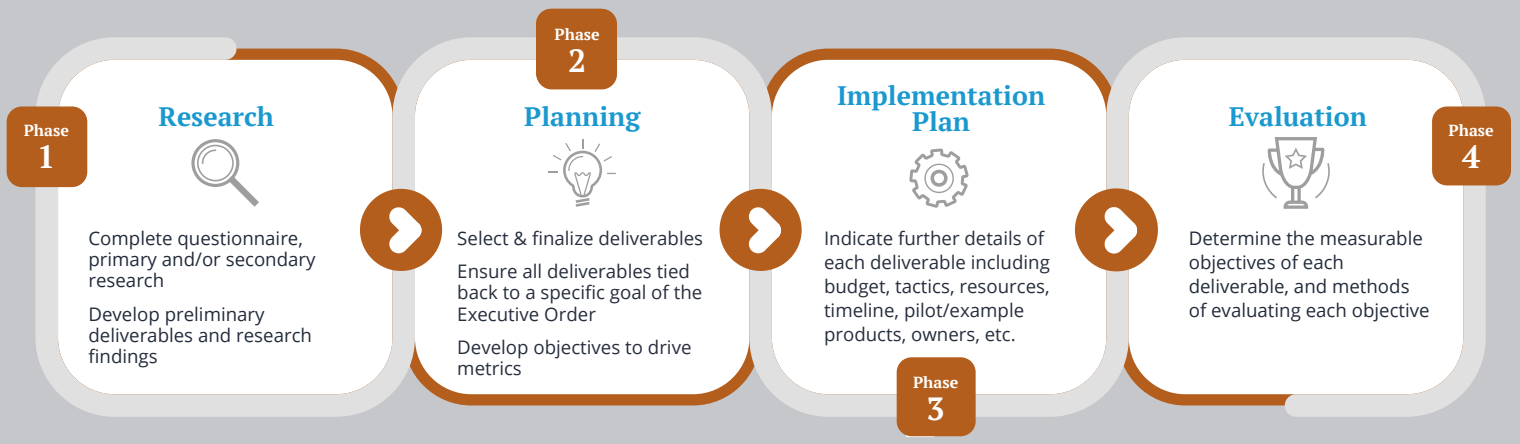



*Figure1: IECC Strategic Breakdown*

## The Council Strategic Phases

To guide the work of the 15 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




In addition, meetings, facilitated discussions, director oversight, shared online platforms, and tools were implemented to avoid duplication of efforts, and to allow for a fully transparent process. 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 indicates the specific deliverables that were 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<br>(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 the Council with required membership.<br>2017-2021 – Council has remained active and has met every quarter and have always met quorum |
| 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 | Passed IECC Charter annually<br>September 2018<br>2018 & 2021 - Submitted final strategic plans 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 and October 2021 - 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 Counterterrorism 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 through October 2021 – 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 | 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 | 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 15 committees and working groups each developed a comprehensive strategic implementation plan that collectively resulted in 68 deliverables and 134 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 combined with a considerable number of donated services, time, and resources from local government entities, academia, and private sector organizations.

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. 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, funding and resources may change as this plan is updated and implemented.

## STATE AND LOCAL GOVERNMENT COMMITTEE

**Deliverable:** Indiana's Cybersecurity Hub Website
- **Objective 1:** IECC will conduct a major review and update of the Cyber Hub website by August 2022.
- **Objective 2:** Increase website traffic to www.in.gov/cyber by 100 percent by September 2023.
- **Objective 3:** Conduct an annual review and update the Cyber Hub website by September of every year.

**Deliverable:** Cyber Emergency Resiliency and Response State Guide – Update
- **Objective 1:** The State of Indiana will update and distribute the Indiana Cyber Emergency Resiliency and Response State Guide by October 2023.

**Deliverable:** Local Officials Cybersecurity Guidebook 2.0
- **Objective 1:** The State and Local Government Committee will update and distribute the Indiana Local Government Cyber Guidebook by May 2023.
- **Objective 2:** The State and Local Government Committee will encourage the downloading of 1,000 Indiana Local Government Cyber Guidebooks by May 2024.

**Deliverable:** Local Government Cyber Engagement Program
- **Objective 1:** The State and Local Government Committee, with the assistance of IECC partners and the National Governors Association, will develop the Local Government Cyber Engagement Program by January 2022.
- **Objective 2:** The State and Local Government Committee, with the assistance of IECC partners and the National Governors Association, will pilot the Local Government Cyber Engagement Program with at least five local government entities by June 2022.

**Objective 3:** The State and Local Government Committee with the assistance of IECC partners will publicly launch the Local Government Cyber Engagement Program by January 2023.
**Objective 4:** As a result of outreach efforts, at least 30 local government entities will have begun using the Local Government Cyber Engagement Program by December 2023.

**Deliverable:** Identity Theft State Roundtable
**Objective 1:** Indiana Department of Workforce Development (DWD) and Indiana Office of Technology (IOT) will lead a round table discussion with other key state agencies about best practices with defending against identity theft and fraud.

**Deliverable:** Local Government Cybersecurity Podcast Series ("Days of Our Cyber Lives")
**Objective 1:** Completion of a 15-minimum episode podcast series on cybersecurity topics for a Hoosier local unit of government audience over the course of one year, available via audio-only (e.g., Apple Podcasts) or video and audio (YouTube) by October 2021.
**Objective 2:** Realizing greater than or equal to 900 combined views & listens for the series by October 2021.

## ELECTIONS COMMITTEE

**Deliverable:** Collaboration with State, Federal, and Sector Communities
**Objective 1:** The new Secretary of State will actively engage with allied organizations indicated in the state's strategic plan by Dec. 31, 2021.
**Objective 2:** The Secretary of State will continue to engage in election cybersecurity collaboration with allied organizations every year as appropriate.

**Deliverable:** Integration of Cybersecurity Professionalism, Awareness, and Practice
**Objective 1:** The Secretary of State will promote integration of experienced, trained, and professionally certified cybersecurity resources into all phases of election administration by November 2024.
**Objective 2:** More than 80 percent of state and local election officials and administrators will be provided ongoing cybersecurity awareness, training, and/or certification opportunities by November 2024.

**Deliverable:** Election Infrastructure Monitoring, Hardening, Testing, and Auditing
**Objective 1:** The Secretary of State will promote election infrastructure monitoring, hardening, testing, and auditing improvements every year until December 2024.

**Deliverable:** Public Engagement and Confidence
**Objective 1:** The Secretary of State will maintain a high level of public engagement in the area of election security and public confidence by November 2024.

**Deliverable:** Continuity, Coordination, Maintenance of Effort and Oversight
**Objective 1:** Indiana Statewide Voter Registration System Core Team will begin formally coordinating and overseeing the deliverables of the IECC Elections Committee Strategic Plan by Dec. 31, 2021.
**Objective 2:** Indiana Statewide Voter Registration System Core Team will assist with all the deliverables and objectives in the IECC Elections Committee Strategic Plan and report the progress to the IECC by Dec. 31 of each year.

## ENERGY COMMITTEE

**Deliverable:** Critical Infrastructure Information (CII)

**Objective 1:** IECC Energy Committee will provide a review of the July 2018 definitions by October 2021.

**Objective 2:** IECC Energy Committee will review potential state policy changes to protect critical infrastructure information while maintaining public access and freedom of information by December 2021.

**Deliverable:** Training

**Objective 1:** Develop a survey to determine whether there are new training needs specific to the energy industry following the Pandemic by October 2021.

**Objective 2:** Identify and recommend opportunities at the state, vocational, or higher education level December 2021.

**Deliverable:** IURC Cybersecurity Forum

**Objective 1:** Indiana Utility Regulatory Commission (IURC) will host a cybersecurity forum for small natural gas utilities to share industry information and best practices by December 2021.

**Deliverable:** Resource Guide

**Objective 1:** The IECC Energy Committee will define emerging technology and supply chain issues related to the grid Qtr. 3 2022.

**Objective 2:** The IECC Energy Committee will determine whether best practices and information are widely available Qtr. 3 2022.

Objective 3: The IECC Energy Committee will develop an industry specific resource guide Qtr. 4 2022.

**Deliverable:** Workplace IT

**Objective 1:** The IECC Energy Committee will develop a survey to identify challenges in the workplace for the energy sector in Qtr. 4 2021.

**Objective 2:** The IECC Energy Committee will identify issues stemming from the work-from-home environment in Qtr. 4 2021.

**Objective 3:** The IECC Energy Committee will share best practices and coordinate with other sectors as needed in Qtr. 1 2022.

## FINANCE COMMITTEE

**Deliverable:** Board Leadership Education Plan

**Objective 1:** IECC Finance Committee will develop a curriculum and identify an instructor(s) to be used for the Board and Executive Leadership Education Plan by June 2022.

**Objective 2:** The Board and Executive Leadership Education will be provided to a pilot group of finance institutions by December 2022.

**Deliverable:** Disruption Plan and Communication Evaluation

**Objective 1:** IECC Finance Committee will develop a Finance Sector Disruption Plan for the State of Indiana by Qtr. 3 of 2023.

**Objective 2:** The IECC Finance Committee will evaluate communication opportunities and identify associated barriers by Qtr. 4 of 2023.

**Deliverable:** Top Security Tips Material 2.0

**Objective 1:** IECC Finance Committee will review and distribute the Top Information Security Tips 2.0 training material for Indiana businesses by December 2022.

## WATER AND WASTEWATER COMMITTEE

**Deliverable:** Cyber Contact List

**Objective 1:** Indiana Department of Environmental Management maintains a cybersecurity contact information for 85 percent of Indiana water and wastewater organizations to be reviewed annually.

**Deliverable:** Cyber Risk Model (Plan) – Update

**Objective 1:** The Water/Wastewater Committee and partners will review and update the Cyber Plan Template for Indiana water/wastewater companies in 2022.

**Objective 2:** Make the updated Cyber Plan Template available online and distribute to water/wastewater utilities by in 2022.

**Deliverable:** Risk Tool

**Objective 1:** Water/Wastewater Committee develops Cyber Assessment Risk Tool within 12 months of securing funding.

**Objective 2:** Make tool available to 80 percent of Indiana AWWA members on AWWA.org for use by Indiana W/WW companies within 12 months of launching.

**Deliverable:** Training Plan

**Objective 1:** Water/Wastewater Committee develop an initial training plan by June 2021 and full training plan within three months of funding.

**Objective 2:** Seventy percent of Indiana water and wastewater companies incorporate the training plan as a part of their operational resources within 24 months of deployment of training plan.

**Deliverable:** Cyber Plan Template – Update

**Objective 1:** IECC Water and Wastewater Committee and partners will distribute the updated Cyber Plan Template to 50 percent of Indiana water and wastewater companies through a variety of methods (including virtual) by March 2022.

**Deliverable:** Water/Wastewater Exercise and Response Education

**Objective 1:** IECC Water and Wastewater Committee and partners will participate in US DHS CISA Exercise August 2021.

**Objective 2:** IECC Water and Wastewater Committee and partners will participate in INNG Hoosier Defender August 2021.

**Objective 3:** Working with partners, develop a water/wastewater virtual workshop launch by October 2021.

**Objective 4:** Promote virtual workshop that result in at least 100 registrants by October 2021.

## COMMUNICATIONS COMMITTEE

**Deliverable:** Establish Voluntary Industry Contact List

**Objective 1:** IECC Communications Committee will develop a form and process to collect a central cyber industry contact list by Qtr. 2 of 2022.

**Objective 2:** Seventy percent of all communications providers complete annual cyber contact form by December 2022.

**Deliverable:** Terminology Glossary – Update

**Objective 1:** IECC Communications Committee will update Communications Sector Terminology Glossary by December 2021.

**Objective 2:** IECC Program Communications Manager will publish the Communications Sector Terminology Glossary to IECC website by January 2022.

**Deliverable:** Broadband and Local Government Education

**Objective 1:** IECC Communications Committee will complete the rural broadband education packages by January 2023.

**Objective 2:** IECC Program Communications Manager will publish the rural broadband education packages by February 2023.

**Objective 3:** Working with identified partners, provide cyber 101 tips for 1,000 individuals and organizations who are learning to operate with high-speed internet by December 2024.

**Deliverable:** Cyber Incident Response Engagement Guide

**Objective 1:** IECC Communications Committee will develop the Communications Sector Engagement Guidance by May 2022.

**Objective 2:** Communications sector partners will distribute the Communications Sector Engagement Guidance to eighty percent of identified industry and key stakeholders by June 2022.

## HEALTHCARE COMMITTEE

**Deliverable:** Long-term Education

**Objective 1:** IECC Healthcare Committee will update Indiana-focused versions of security education in 2022.

**Objective 2:** IECC Healthcare Committee and partners will provide updated Indiana-focused versions of security education to 80 percent of Indiana healthcare providers in 2022.

**Objective 3:** IECC Healthcare Committee and partners will collect customer effectiveness, usage, and/or feedback survey for future development in 2023.

**Deliverable:** "Healthcare Cyber in a Box"

**Objective 1:** IECC Healthcare Committee will create a "Healthcare Cyber in a Box" of security education designed for small- to medium-size offices and systems in 2022.

**Objective 2:** Healthcare Committee and partners will distribute Healthcare Cyber in a Box of security education information to 80 percent of Indiana healthcare providers.

**Objective 3:** IECC Healthcare Committee and partners will measure feedback/usage of the toolkit by 2023.

**Deliverable:** Vendor Management - Healthcare IT Security, Risk & Compliance Handbook

**Objective 1:** IECC Healthcare Committee will draft the initial document including key outline of processes and procedures Indiana providers need to implement by Qtr. 1, 2022.

**Objective 2:** Circulate the document among the IECC Healthcare Committee for revisions and edits by Qtr. 2, 2022.

**Objective 3:** Implement Committee feedback and finalize document by Qtr. 2 of 2022.

**Objective 4:** Publish final draft on the Indiana Cybersecurity website by Qtr. 3 of 2022.

**Deliverable:** Exercise

**Objective 1:** Working with partners, participate in a statewide cyber exercise that affects healthcare industry by August 2021.

**Objective 2:** Working with partners, participate in an exercise with the National Guard at Muscatatuck by August 2021 that addresses a known cyber vulnerability.

**Deliverable:** Cyber Sharing Platform

**Objective 1:** IECC Healthcare Committee will beta test with the Cyber Awareness and Sharing Working Group by Qtr. 1 2022.

## DEFENSE INDUSTRIAL COMMITTEE

**Deliverable:** Cyber Market System

**Objective 1:** IEDC Defense Development and partners will review the current cybersecurity market pursuit plan and system in 2021.

**Deliverable:** Cyber Digital Platform

**Objective 1:** IEDC Defense Development and partners will develop a pilot of the Indiana defense cybersecurity market development and capture plan and system (Digital Platform) by 2021.

**Objective 2:** Indiana increases to two percent (about $300M) of the Department of Defense (DOD) cybersecurity market share ($15B plus) by FY 2025.

**Deliverable:** Cyber Statewide Testbed

**Objective 1:** Establish a nationally recognized cybersecurity test bed in Indiana by June 2021.

**Objective 2:** Indiana captures five percent of international cybersecurity market share of cybersecurity test, training, and demonstration plan and capability by December 2025.

**Deliverable:** Cybersecurity Capability Maturity Model (CMMC) Program

**Objective 1:** IEDC and partners will develop a Cybersecurity Capability Maturity Model (CMMC) framework in Indiana by December 2021.

**Objective 2:** IEDC and partners will promote Cybersecurity Capability Maturity Model (CMMC) in Indiana to 80 percent of key stakeholders and associations by January 2022.

## ECONOMIC DEVELOPMENT COMMITTEE

**Deliverable:** Investment

**Objective 1:** The Economic Development Committee with the IEDC will develop an economic development support framework for Indiana companies to thrive in the cybersecurity landscape by December 2022.

**Objective 2:** Companies that move, start, or grow here will have a framework for economic development support by December 2023.

**Deliverable:** Leadership

**Objective 1:** Indiana Economic Development Corporation and Committee will work to identify potential partners, activities, and initiatives of cybersecurity influencers in the State of Indiana by December 2022.

**Objective 2:** Measure the effectiveness of IEDC supported activities and initiatives in the cybersecurity space by December 2023.

**Deliverable:** Technical Assistance

**Objective 1:** IEDC and partners will develop a cybersecurity technical assistance plan in Indiana by January 2022.

**Objective 2:** Measure the effectiveness of the Cybersecurity technical assistance plan by the number of participants (40) by February 2023.

## WORKFORCE DEVELOPMENT COMMITTEE

**Deliverable:** Enhance CyberseekIN.org Data Tool - Workforce Pillar

**Objective 1:** Indiana DWD add Credential Engine certifications data to CyberseekIN.org (training providers) by June 2022.

**Objective 2:** Indiana DWD continue Data enhancements to CyberSeekIN.org including continual updates to training providers, Apprenticeship Data/Opportunities, and Promote opportunities, training, events surrounding cybersecurity in Indiana by October 2022.

**Deliverable:** Cybersecurity Talent Pipeline and Job Openings Dashboard - Workforce Pillar

**Objective 1:** Indiana Department of Workforce Develop will create cybersecurity workforce dashboard metrics – measuring Indiana's job demand, talent pipeline, apprenticeships, and training opportunities by January 2022.

**Deliverable:** K-12 Cybersecurity Content - K-12 Pillar

**Objective 1:** Governor's Workforce Cabinet with support from IDOE will develop and promote a high school CTE Program of Study in Cybersecurity by June 2022.

**Objective 2:** Indiana Department of Education will develop a menu of cybersecurity-related professional development and resources, including K-12 computer science offerings, by June 2022.

**Objective 3:** Indiana Department of Education and Cybersecurity Program Director will edit and distribute the Cybersecurity for Education Toolkit 2.0 by February 2022.

**Deliverable:** Promote Cybersecurity Training Across the K-12 Sector to Protect the Educational Process - K-12 Pillar

**Objective 1:** The joint Cybersecurity Task Force ensure more than 75,000 staff and students are delivered training and phishing support through the KnowBe4 platform by December 2024.

**Objective 2:** The joint Cybersecurity Task Force will raise awareness of schools to digital threats to the educational process by raising awareness through monthly newsletters, and by working with partners to provide professional development for school IT staff by December 2024.

**Objective 3:** DOE will work to encourage all schools to appoint one staff member to monitor information releases from the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Indiana Information Sharing and Analysis Center (IN-ISAC) by December 2023.

**Objective 4:** Create a DOE Moodle Community to share school cybersecurity information with public, religious, and private schools as well as provide opportunities for secure collaboration and sharing of best practices by December 2021.

**Deliverable:** Update Cyber Program Data Tool (CHE) - Higher Education Pillar

**Objective 1:** Commission for Higher Education will re-launch survey/tools to capture and collect program course curriculum to help the IECC understand and inventory which higher ed schools are providing cybersecurity related training programs by December 2021.

**Objective 2:** Commission for Higher Education will update the Cyber Program Data Tool and Report by March 2022.

## PRIVACY WORKING GROUP

**Deliverable 1:** Indiana PII Guidebook

**Objective 1:** IECC Privacy Working Group update the Indiana PII Guidebook for government and general public by the end of April 2022.

**Deliverable 2:** Indiana Privacy Toolkit

**Objective 1:** IECC Privacy Working Group develop an Indiana Privacy Toolkit for the Indiana business community, public sector, and local government by July 2022.

**Objective 2:** At least 200 users have accessed/downloaded the Indiana Privacy Toolkit for the Indiana business community, public sector, and local government by April 2023.

## CYBER AWARENESS AND SHARING WORKING GROUP

**Deliverable:** Public Relations Campaign Plan - Update

**Objective 1:** The IECC Communications Program Manager will use the 2018 Statewide PR Cybersecurity Campaign Plan and develop a phased approach to the tactics as resources allow by December 2021.

**Objective 2:** IECC Communications Program Manager will leverage the assets of Indiana's cybersecurity program to create an increasingly larger presence on social media channels including Twitter, Facebook, and LinkedIn increasing its subscription by 30 percent each fiscal year.

**Objective 3:** The IECC Communications Program Manager will utilize a weekly blog as a tool for measurably increasing public awareness by further positioning Indiana as a leader in cybersecurity and increasing its subscription by 25 percent each fiscal year.

**Deliverable:** Inventory of Cyber Sharing Resources

**Objective 1:** IECC Cyber Awareness and Sharing Working Group will complete an inventory of cyber sharing resources by August 2021.

**Deliverable:** MS-ISAC Member Recruitment

**Objective 1:** Indiana-ISAC will work to increase MS-ISAC membership by 25 percent each calendar year.

**Deliverable:** Best Practices

**Objective 1:** IECC Cyber Awareness and Sharing Working Group will update a list of best practices by July 2022.

**Deliverable:** Cyber Sharing Maturity Model

**Objective 1**: IECC Cyber Awareness and Sharing Working Group will edit and post the Indiana's updated cyber sharing maturity model by July 2022.

**Objective 2:** ECC Cyber Awareness and Sharing Working Group will distribute Indiana's updated cyber sharing maturity model to critical infrastructures through ninety percent of Indiana associations by August 2022.

**Deliverable:** Cyber Sharing Community - Slack Channel

**Objective 1:** IECC Cyber Awareness and Sharing Working Group will create the Slack Channel by May 2021.

**Objective 2:** IECC Cyber Awareness and Sharing Working Group and IECC Healthcare Committee will conduct a beta test of the Slack Channel by December 2021.

**Objective 3:** Complete the Live Production Launch of the Slack Channel by January 2022.

## CYBER RESILIENCY AND RESPONSE WORKING GROUP

**Deliverable:** State Cyber Exercises

**Objective 1:** The State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Table Top Exercise by August 2021.

**Objective 2:** IECC will work with INNG to incorporate a cyberattack into a natural disaster exercise during the Homeland Defender Exercise by August 2021.

**Objective 3:** The State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Operational Exercise by 2023.

**Deliverable:** Cyber Emergency Education to Local Law Enforcement

**Objective 1:** ISP and Cybersecurity Program Director work to develop the Cyber Emergency Response Education for Local Law Enforcement by May 2022.

**Objective 2:** ISP and IECC partners distribute the Cyber Emergency Response Education to 80 percent of Local Law Enforcement by June 2022.

**Deliverable:** Emergency Manager Cybersecurity Toolkit 3.0

**Objective 1:** IECC Emergency Services and Exercise Working Group will update the Emergency Manager Cyber Response Toolkit 3.0 by March 2022.

**Objective 2:** IDHS will launch a workshop using the Emergency Manager Cyber Response Toolkit 3.0 by April 2022.

**Deliverable:** Cyber Annex and Cyber Liaison

**Objective 1:** IDHS will edit and distribute the IDHS Cyber Annex to appropriate parties by Qtr. 3 of 2022.

**Objective 2:** IDHS and IECC partners will exercise the IDHS Cyber Annex with the cyber liaisons by December 2023.

**Deliverable:** INNG Cyber State Capabilities

**Objective 1:** The Indiana National Guard will inform state leadership of their cyber response capabilities to a statewide cyber emergency when directed by a federal disaster declaration or ordered to State Active Duty by the Governor by December 2024.

## LEGAL AND INSURANCE WORKING GROUP

**Deliverable:** Cyber Insurance Toolkit

**Objective 1:** IECC Legal and Insurance Working Group will develop a Cyber Insurance Toolkit to be provided to government and businesses by April 2022.

**Objective 2:** With an effective communications plan, point more than 1,000 users access the Cyber Insurance Toolkit by December 2023.

**Deliverable:** Policy Review

**Objective 1:** Legal and Insurance Working Group will review and distribute a list of cyber laws applicable to Indiana businesses and residents under the current landscape every year in December.

**Deliverable:** Funds Transfer Fraud Fact Sheet

**Objective 1:** IECC Legal and Insurance Working group will develop a Funds Transfer Fraud Fact Sheet to be provided to government and businesses by January 2022.

**Deliverable:** Cyber Insurance Survey - Post-Covid

**Objective 1:** Legal and Insurance Working Group with Indiana University will conduct a post-COVID survey of businesses for insurance coverage and cybersecurity insurance coverage by June 2022.

**Objective 2:** IECC Legal and Insurance Working Group with Indiana University will provide a report of the findings of the cyber insurance survey to the IECC by September 2022.

## STRATEGIC RESOURCE COMMITTEE

**Deliverable:** Policy Research Report

**Objective 1:** IECC and partners will update a report of state and federal cybersecurity legislation by December 31, 2022.

**Deliverable:** IECC Scorecard 2.0

**Objective 1:** IECC, along with Indiana State University and Purdue University, will develop a Scorecard 2.0 with a Level Up Guide to improve cybersecurity posture by January 2022.

**Objective 2:** IECC will pilot Indiana's Cybersecurity Scorecard 2.0 with Level Up Guide with local governments by July 2022.

**Objective 3:** IECC will relaunch Indiana's Cybersecurity Scorecard 2.0 with Level Up Guide to the public by December 2022.

**Deliverable:** Indiana Cyber Success Report (2017-2021)

**Objective 1:** The Indiana Executive Council on Cybersecurity will develop a report to address the status and successes of the IECC as well as Indiana organizations by October 29, 2021.

**Deliverable:** IECC 2021 Strategic Plan

**Objective 1:** IECC will develop a 2021 Strategic Plan for the Council by October 29, 2021.

**Deliverable:** Outreach to Underrepresented Sectors

**Objective 1:** With key partners, identify cybersecurity awareness needs in additional Indiana industries (manufacturing, transportation, small business, and agriculture) by December 2022.

**Objective 2:** Provide industry contacts with education materials and set up a regular communication cadence for each industry by March 2023.

## Observations and Considerations of the IECC

Defining cybersecurity—and efforts to protect against cybersecurity threats—must be illustrated in a way that is simple yet effective, complete yet attainable. Although cybersecurity has a lot of ins, a lot of outs, a lot of what-have-yous with a lot of strands to keep in our heads, it must be demystified. 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 towards a multi-disciplinary solution to deal with such an extensive threat. It must encompass not only government at all levels, but Indiana businesses at all levels and sized, and, indeed, all Hoosiers, if it is to be effective. 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. The cyber threat is a dynamic environment. Instead, effective cybersecurity is best understood through a lens of evidence-based risk reduction.

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 ubiquitous threat it poses to all Hoosiers, which is why the Governor and state lawmakers continue to champion its importance. As with many important issues, the success of a cybersecurity strategy depends on the resources and funding available to support its implementation. It is also important to note that while these implementation plans have estimated time frames, budgets, and resources, they are agile in nature and will be updated as progress and corrections are driven by the expertise of the members on those committees and working groups.

It is imperative that the Council remains agile, 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. As many of these deliverables are being implemented, their nature and scope may change commensurate with the participants who are advising on them and the ever-evolving cyber landscape. The Council will continue to 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.

# 2021 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 where 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 the development of local government cybersecurity resources and education;
- Providing necessary support to the critical infrastructures as they move forward with their many deliverables This includes planning, training, and exercising in preparation of a cyberattack (e.g. working with small operators in safe environments such as Muscatatuck).
- 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 supporting the necessary cybersecurity experts, tools, and service providers as the cyber threat continues to evolve.


# Part 3
# Real People, Real Work

## 2018-2021 Membership and Leadership

Since its first strategic plan in 2018, the Council has been supported by more than 200 members consistently each year. Of those, Voting and Advisory Members were selected to lead the 15 committees and working groups. For a full list of the members and committee and working group leadership from 2018 - 2021, see Appendix E. It is important to note that while members have come and gone due to job changes, life changes, etc., every member has been a significant reason why the Council has been so successful.

## Council Stats

### 2018

**214** Members

**22 of 69** Deliverables Completed

**42** of **120** Objectives Completed

### 2019

**256** Members

**17 of 69** Deliverables Completed

**36** of **120** Objectives Completed

### 2020

**246** Members

**8 of 69** Deliverables Completed

**9** of **120** Objectives Completed

### 2021

**238** Members

**7 of 69** Deliverables Completed

**93** of **120** Objectives Completed

### Total

**350+** Members

**54 of 69** Deliverables Completed

**93** of **120** Objectives Completed

# Best Practices of the IECC

The Council has accomplished an unprecedented amount of work for the citizens and businesses of Indiana in the last four years 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 achieved by working 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.

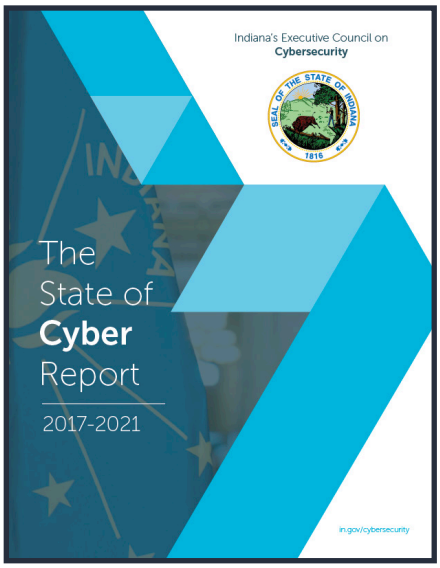
When leadership is asked about what makes the IECC so unique and successful, the following best practices are shared:

- **Culture is everything.** Culture of the Council has always centered around empowerment of all our members and partners. No one entity owns cybersecurity. The state is a key facilitator but puts a lot of trust in the subject matter experts. No one needs to ask permission to do a cyber initiative. They are the experts. If a sector that is not the state feels that based on their research a particular initiative should happen, the state does not question their expertise. Instead, the state does its best to support their efforts as they lead and complete it.
- **Variety is the key ingredient to success.** The wide variety of the subject matter experts who drive the Council's innovative thinking and execution of initiatives come from public, private, academic, and military industries. But one representative on the council will not provide you the breadth and depth of viewpoints needed for a successful plan. It is important to have regional representatives (north, central, and southern Indiana) in all the committees and working groups as well as small, medium, and large entities in that sector to ensure that diverse input is provided in developing strategic plans.
- **A neutral program director.** The State of Indiana hired its first fully dedicated cybersecurity program director in March 2017 to develop the strategic framework and facilitate the Council in fulfilling its purpose. Having a director whose primary objective is not one agency's mission, but the Governor's Executive Order, has assisted the director to really understand and better represent the state as a whole instead of just one agency. It has also been beneficial that the director is not a project manager or a technologist, but is an executive who understands how government, private sector, military, and academia works with first-hand experience; respects and understands the politics (big and small) but is not political; and is a proven business strategist and effective communicator.
- **State agencies work together.** For the better part of a decade the Chief Information Officer (CIO) of the State and the Executive Director of the Indiana Department of Homeland Security have been working hand-in-hand on cybersecurity. There is not one agency in charge. In fact, much of what Indiana has done is seek to understand every agency's role in cybersecurity and embrace it within the process, not fight about it. When agencies are heard and respected, they are more willing to come to the table. This has been true with the state agencies on the Council. It is also important that the Governor has encouraged this collaboration because that is the only way we can be successful as a state.
- **Set expectations early and often.** Every year the Council reviews the membership and the Charter. And every year, the Council leadership ensures that the members are aware of the time expectations, the deadlines, the priorities, and the challenges to problem solve together. That is why meeting quarterly as a whole Council is important to its communication efforts and success.

- **Templates are key.** With so many committees and working groups and so many executives providing a volunteer service, providing templates to guide discussions and communicate what each team is doing is important to the organization, effectiveness, and efficiency of the Council.
- **Respect time.** From the beginning, it was made very clear that if a member felt like a meeting was a waste of time to be open about that frustration and the program director will see what can be improved. Being respectful of every member's time as well as making sure that when they attend a meeting, they feel excited to be a part of something that is helpful to others is a point of reference to be checked on a consistent basis. This is why it is believed all the meetings are still very well attended.
- **Be flexible.** Recognizing that we have a plan with set dates and objectives is important to every executive on the Council, but also recognizing that things happen (like a worldwide pandemic) and there is no failure is shifting things around and pausing initiatives because members are working 50-70 hours at their full-time jobs. Also being clear from the beginning of every plan that things will happen, people will change jobs or need to step away and objectives may need to be updated is also okay and not deemed a failure. In fact, even with all that has happened over the last couple of years, the Council still completed a majority of their deliverables. That is the true success.
- **Be transparent.** If all members have access to many of the inner workings of the planning and implementation of each plan, then there are never questions of impropriety or assumptions that are not correct, which in many cases can distract from what we are trying to accomplish. Since 2017, there has never been an issue raised because everything is there for members to see. And if they have questions, the Director will have transparent conversations of any possible concerns there may be.

## No Smoke and Mirrors Here…

Each committee and working group followed the four-step strategic process (research, planning, implementation, and evaluation). This process provides Indiana a very accurate understanding of the many challenges facing the state, as well as the many current and possible solutions that can enhance cybersecurity at all levels. Through work of these committees, there is not just talk on how to protect Indiana from cyber threats, but there are actual plans followed by action.




In 2018, the Council submitted to the Governor a strategic plan that to some may have been too aggressive and, with a strategic framework that had never been used in the nation. And while there were those who were not sure how this complex ecosystem approach would work, the Council not only completed 78 percent of its total 69 deliverables, and 77 percent of the 120 objectives, but has seen some tremendous successes outside the Council as well.

So many private, public, academic, and military organizations along with individuals who just want to make a difference in cybersecurity have succeeded where others have not. It is an honor to be the state that supports these endeavors whether directly with the Council or from afar with acknowledgment. To learn more about the successes of the *2018 Indiana Cybersecurity Strategic Plan* and other accomplishments of cyber warries in our state, read the "2021 State of Cyber Report" found at www.in.gov/cybersecurity.

## 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. Council membership also will be reviewed and recruitment of experts in the fields will be ongoing.

The Council also will continue to provide 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.

The goal of the Council is to move cybersecurity to the *Next Level* in Indiana. However, we must do this 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. By providing resources to those organizations who need it most 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 Indiana. With the continued guidance and support of experts throughout the State of Indiana, Hoosiers will continue to be safer, and businesses will continue to thrive.

# Appendices

- Appendix A Indiana Executive Council on Cybersecurity - Executive Order
- Appendix B Indiana Executive Council on Cybersecurity - Charter
- Appendix C Indiana Executive Council on Cybersecurity – Phase Forms
- Appendix D Indiana Executive Council on Cybersecurity – Committee and Working Group Implementation Plans
  - D. 1 Communications Committee
  - D. 2 Defense Industrial Committee
  - D. 3 Economic Development Committee
  - D. 4 Elections Committee
  - D. 5 Energy Committee
  - D. 6 Finance Committee
  - D. 7 State and Local Government Committee
  - D. 8 Healthcare Committee
  - D. 9 Water and Wastewater Committee
  - D. 10 Workforce Development Committee
  - D. 11 Resiliency and Response Working Group
  - D. 12 Cyber Awareness and Sharing Working Group
  - D. 13 Legal and Insurance Working Group
  - D. 14 Privacy Working Group
  - D. 15 Strategic Resource Working Group
- Appendix E Indiana Executive Council on Cybersecurity – Membership and Leadership Lists

# Appendix A

## Indiana Executive Council on Cybersecurity - Executive Order

# 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: May 7, 2021

Version: 6

# Table of Contents

## 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 cybersecurity.

- 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 state's 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 Cybersecurity and Infrastructure Security Agency (CISA)(formerly National Protection and Programs Directorate); and

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

Additional Voting Members may be appointed at the discretion of the Governor (e.g., Lt. Governor Office, Secretary of State, local government representations, etc.).

## 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 strategic 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) designees 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 and Cybersecurity Program Director.

- 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 Advisory 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.

## Section III: Location of Meetings

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

- Council meetings shall be held primarily 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.

- When in-person meetings are being held, attending meetings by conference call or online usage may be 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 designees vote on their behalf.

### Section VI: Delegation of Authority

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

- The Council Chair may delegate in writing at his or her discretion his or her 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:
    - State and Local Government Committee
    - Finance Committee
    - Energy Committee
    - Water and Wastewater Committee
    - Communications Committee
    - Healthcare Committee
    - Defense Industrial Committee
    - Elections Committee
    - Economic Development Committee
    - Workforce Development Committee
    - Privacy Working Group
    - Cyber Awareness and Sharing Working Group
    - Resiliency and Response Working Group
    - Legal and Insurance 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

- 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, unless approved by the Chair. 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 quarterly, 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 Microsoft Teams. 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 a.m. and 4:30 p.m., 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 its handling instructions as appropriate.

- The Council may receive sensitive law enforcement information from the Indiana State Police, 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 and must abide by its handling instructions as appropriate.

- Council Members who release such information to external parties without prior approval are subject to immediate dismissal from the Council and any other legal consequences as appropriate.

## 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
## IECC 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 RomeroCLM@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

---

**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 are 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 sta~~keholders 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**

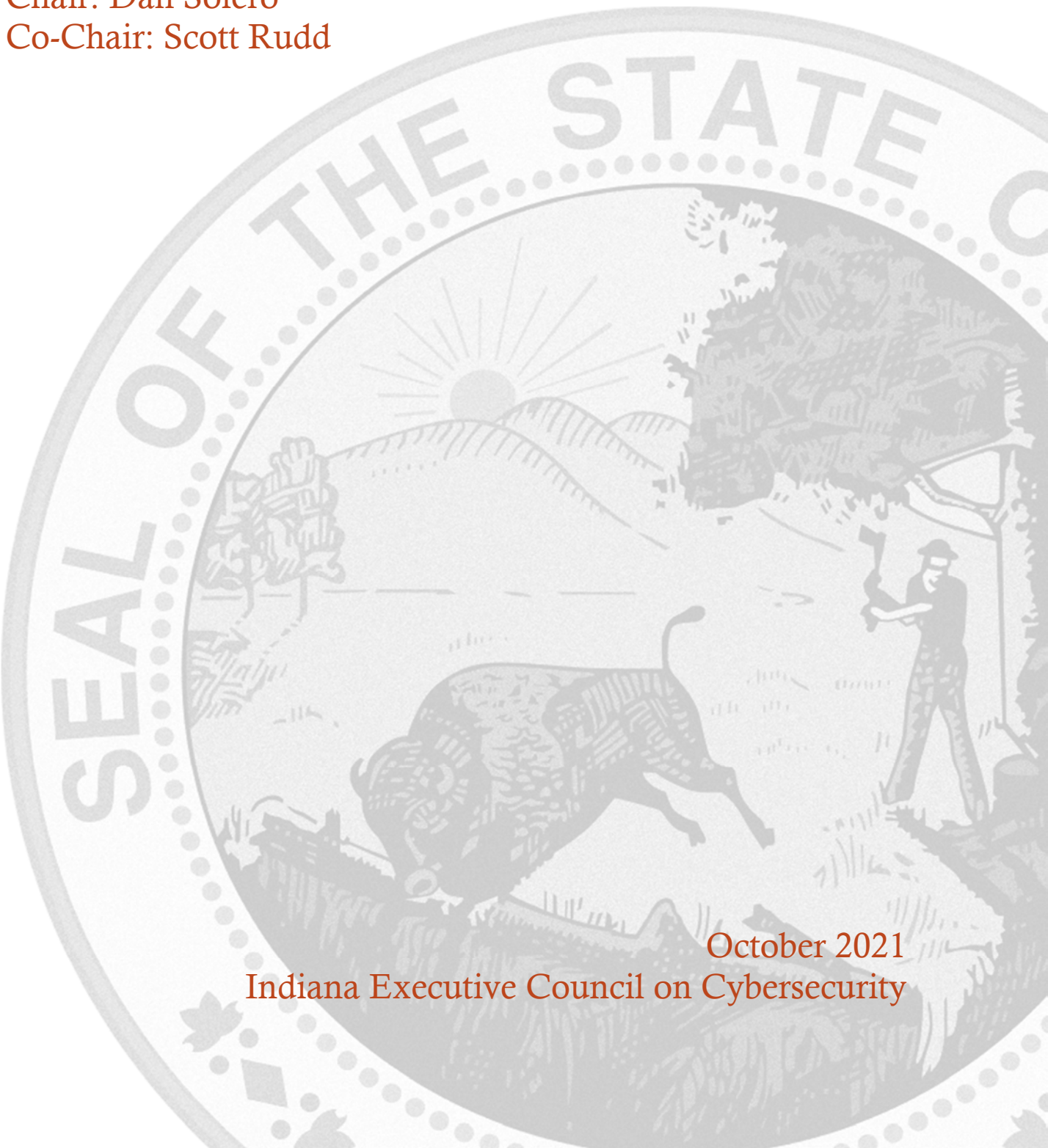
# Appendix D

## IECC Committee and Working Group Implementation Plans


# Appendix D.1
## Communications Committee

# COMMUNICATIONS COMMITTEE STRATEGIC PLAN

Chair: Dan Solero
Co-Chair: Scott Rudd




October 2021
Indiana Executive Council on Cybersecurity

# Communications Committee
# Strategic Plan

# Table of Contents

# Committee Members

# Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Cochrane | Douglas | Integrated Public Safety Commission | Director of Network Services | As Needed |
| Dignin | Kelly | Integrated Public Safety Commission | Executive Director | Full Time |
| Foltz | Jeremy | Tech Mahindra | Developer – Team Lead | Full Time |
| Greene | John | New Lisbon Telephone Company | CEO | Full Time |
| Hart | Joni K | Broadband Innovation Group | Executive Director | As Needed |
| Korty | Andrew | Indiana University | CISO | Full Time |
| Krebs | Victoria | AT&T | Professional Cybersecurity | Full Time |
| Moorhead | Philip | Ivy Tech Community College | Adjunct Professor | As Needed |
| Reuter | Ed | Indiana Statewide 911 Board | Executive Director | Full Time |
| Rudd | Scott | President | Rudd Consulting, LLC | Co-Chair |
| Salahieh | Rami Maximus | Ivy Tech Community College, Valparaiso, NIISSA | CSIA Program Chair, CSOC Valpo Director | Full Time |
| Solero | Dan | AT&T | AVP - Cybersecurity | Chair |
| Terrell | Alan | Indiana Rural Broadband Association | President | As Needed |

| | | | | |
|---|---|---|---|---|
| Lehigh | Keith | Indiana University | Chief Information Security Officer | As Needed |
| Fay | Sally | IPSC-SWIC | Director of Communications-Coordinator | As Needed |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan.*

For more information, visit www.in.gov/cybersecurity.

# 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**
  - Voluntary Industry Contact List
  - Terminology Glossary
  - Cyber Incident Response Engagement Guide
  - Broadband and Local Government Education

- **References**
  - DHS Critical Infrastructure Sector-specific Overview: https://www.dhs.gov/communications-sector
  - DHS 2015 Sector-specific Plan: 2015 Sector-Specific Plans | CISA
  - National Council of ISACs: MEMBER ISACS | natlcouncilofisacs (nationalisacs.org)
  - 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: OUCC: Utility Website Links
  - National Center for Systems Security and Information Assurance (CSSIA): Home - CSSIA: NSF ATE Center
  - CyberSeek.org: Cybersecurity Supply And Demand Heat Map (cyberseek.org)
  - Indiana Utility Regulatory Commission: https://www.in.gov/iurc/
  - Federal Communications Commission: https://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 activity. 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 occur 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. For responses to proliferate through the sector at the speed of an attack, organizations must be made to feel empowered to act 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: 2015 Sector-Specific Plans | CISA
    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: Centers of Academic Excellence in Cyber Operations (nsa.gov)
    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. DePaul University Cyber Club is a leader in Cyber Security Competition: DeBuzz | Sections | DePaul University Newsline | DePaul University, Chicago
    c. 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?** Recommendations are as follows:
    - This committee does not know of any schools in Indiana that are a CAE Center of Academic Excellence in Cyber Operations. Indiana has no CAE in CO yet. Please see the list below for the entire USA: Centers of Academic Excellence in Cyber Operations (nsa.gov)
    - This committee does 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/
    - There is a 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, there is a 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/
- This committee recommends that the state must make it a mandatory part of our College Education in Indiana for students attending college to take a course in cybersecurity awareness.

**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. 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:
b. According to CyberSeek.org, it shows that the supply of cybersecurity workers in Indiana is at Very Low with cybersecurity workforce Supply/Demand Ratio at 2.5 with a total of 4,119 cybersecurity job openings (Oct. 2021) and a total employed cybersecurity workforce of 10,336.

**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: 2015 Sector-Specific Plans | CISA
    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): National Council of ISACs (nationalisacs.org)
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: Establish Voluntary Industry Contact List

# Deliverable: Establish 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?**
   ☒ 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?**
   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?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. Indiana Public Safety Commission
    d. Indiana Rural Broadband Association
    e. Satellite Industry Association
    f. Indiana Exchange Carrier Association
    g. Other companies and organizations in the communications sector

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

13. **What are the expected challenges to completing this deliverable?**
    a. Getting to 80%+ coverage for contacts and keeping information up to date will be the biggest challenge. We are exploring ways to tie this into other government records of the same nature that have update procedures defined.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Research Contact Points/Structure | Scott Rudd | 50 | Qtr. 1 2022 | Reset all targets due to gap in program |
| Design Survey | Scott Rudd | 50 | Qtr. 1 2022 | |
| Review/Survey Appropriate Housing of Data Collected | Scott Rudd | 25 | Qtr. 1 2022 | |
| Provide Draft Survey to Sector Members | Scott Rudd | 25 | Qtr. 2 2022 | |
| Assign Members to assist with subsector response | Scott Rudd | 25 | Qtr. 2 2022 | |
| Assign Members to research other state data points | Scott Rudd | 25 | Qtr. 2 2022 | |
| Survey Response Deadline | Scott Rudd | 95 | Qtr. 4 2022 | |
| Prepare List for Committee Review | Scott Rudd | 0 | Qtr. 4 2022 | |
| Finalize Deliverable | Scott Rudd | 0 | Qtr. 4 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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?**

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 are 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 79%

**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. To Be Determined

## 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 negatively affect this deliverable.

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

☒No ☐ Yes

**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. Integrated Public Safety Commission (IPSC) and industry associations

**27. Can this deliverable be used by other sectors?**

☒No ☐ Yes

## Communications

---

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

a. Indiana Office of Technology (IOT) and Integrated Public Safety Commission (IPSC)

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

☒No ☐ Yes

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

a. None

## *Evaluation Methodology*

**Objective 1:** IECC Communications Committee will develop a form and process to collect a central cyber industry contact list by Qtr. 2 of 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

**Objective 2:** Seventy percent of all communications providers complete annual cyber contact form by December 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: Terminology Glossary

# Deliverable: Terminology Glossary Update

## *General Information*

1. **What is the deliverable?**
   a. Terminology Glossary Update

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?**
   ☐ 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?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. Scott Rudd

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?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

## 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 | Scott Rudd | 50 | November, 2021 | |
| Publish release 2 of paper to IECC website | Scott Rudd | 0 | December, 2021 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| 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 greatest benefit to the glossary is 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 are 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 the comparable jurisdictions (e.g., other states) that have similar projects that we can compare this project to using the same metrics?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

## 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?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. IT
b. 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)?**

☐No ☒ Yes

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

a. Not at this time.

## *Evaluation Methodology*

**Objective 1:** IECC Communications Committee will update Communications Sector Terminology Glossary by December 2021.

*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 Program Communications Manager will publish the Communications Sector Terminology Glossary to IECC website by January 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: Broadband and Local Government Education

# Deliverable: Broadband and Local Government Education

## *General Information*

1. **What is the deliverable?**
   a. Broadband and Local Government Education

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?**
   ☐ 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 product is intended to provide basic cyber hygiene, privacy, and security guidance to consumers and small business users of new high speed rural broadband services, to safely use newly deployed modern communications infrastructure.

6. **What metric or measurement will be used to define success?**
   a. Creation or curation of educational content
   b. Peer review of content for efficacy and appropriateness
   c. Publication of materials to the IECC website

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Any user of broadband technologies can benefit, though the target audience is users of newly deployed rural broadband services

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 content

12. **Who should be main lead of this deliverable?**
    a. Rami Maximus Salahieh

13. **What are the expected challenges to completing this deliverable?**
    a. Curating meaningful and helpful content will require feedback from the target audience. Focus group execution may be present technical challenges as COVID 19 remains a factor in establishing group settings.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Phase 1 research | Rami Maximus Salahieh | 10 | October, 2021 | |
| Phase 2 development | Rami Maximus Salahieh | 0 | December 2021 | |
| First iteration complete | Rami Maximus Salahieh | 0 | December 2021 | |
| Assign sections to committee members for review | Rami Maximus Salahieh | 0 | January 2022 | |
| Review completed first iteration | Rami Maximus Salahieh | 0 | February 2022 | |
| Establish and run focus groups for target audience feedback | Rami Maximus Salahieh | 0 | March 2022 | |
| Revise content based on feedback and edit for flow and grammar | Rami Maximus Salahieh | 0 | April 2022 | |
| Publish release 1 to IESS website | Rami Maximus Salahieh | 0 | May 2022 | |

## 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 |
|---|---|---|---|---|---|---|
| No Response | | | | | | |

## Benefits and Risks

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

a. The greatest benefit to educate new users of rural broadband in the areas of security best practices for safety and privacy.

18. **How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?**
    a. Security awareness is a fundamental pillar of security programs. This extends to broadband users to that they are equipped to resist cybercrime and stay safe online.

19. **What is the risk or cost of not completing this deliverable?**
    a. The biggest risk is that an under educated user base may be more vulnerable to data loss, privacy incursions, and cyberattack.

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 audience reviewed content. (This is a binary metric. Completion and publication = success)
    b. Engagement from the target audience will also be used to gauge success. A good baseline for engagement metrics will be established based on the form and delivery mode of the content.

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. There are many education content creation and delivery efforts across all sectors. It is unknown whether other states are curating security content specifically aimed at the growing user base of rural broadband services.

## 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?**
    ☒No ☐ Yes

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?**

☐No ☒ Yes

a. IT
b. Public Safety

## Communications

---

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

a. Industry associations and consumer groups

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

☐No ☒ Yes

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

a. Copyrights and rights to use any third-party content will need to be reviewed before publication to the IECC website.

## *Evaluation Methodology*

**Objective 1:** IECC Communications Committee will complete the rural broadband education packages by January 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

**Objective 2:** IECC Program Communications Manager will publish the rural broadband education packages by February 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

**Objective 3:** Working with identified partners, provide cyber 101 tips for 1,000 individuals and organizations who are learning to operate with high-speed internet by December 2024.

*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

# Deliverable: Cyber Incident Response Engagement Guide

# Deliverable: Cyber Incident Response Engagement Guide

## *General Information*

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

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?**
   ☐ 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 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?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. Resiliency and Response 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. 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. Kelly Dignin

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?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Phase 1 questionnaire | Kelly Dignin | 10 | November, 2021 | Updating from 2018 |
| Phase 2 questionnaire | Kelly Dignin | 0 | December, 2021 | Updating from 2018 |
| Research similar engagement guidance documents from adjacent sectors or similar projects | Kelly Dignin | 0 | November, 2021 | |
| Draft document outline | Kelly Dignin | 10 | December, 2021 | |
| Assign sections to committee members for authorship | Kelly Dignin | 0 | December, 2021 | |
| Review completed first draft document sections for content | Kelly Dignin | 0 | January, 2022 | . |
| Submit reviewed draft document broadly to industry groups, subject matter experts, and peer sectors for comment. | Kelly Dignin | 0 | February, 2022 | |
| Revise document based on feedback and edit for flow and grammar | Kelly Dignin | 0 | March 2022 | |
| Publish release 1 | Kelly Dignin | 0 | March, 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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 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 are 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?**

☒No ☒ Yes

**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?**

☒No ☐ Yes

## 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?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. IT
b. 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)?**

☒No ☐ Yes

a. 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. No Response

## *Evaluation Methodology*

**Objective 1:** IECC Communications Committee will develop the Communications Sector Engagement Guidance by May 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

**Objective 2:** Communications sector partners will distribute the Communications Sector Engagement Guidance to eighty percent of identified industry and key stakeholders by June 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

# 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 1.0

# IECC Communications Committee
# Telecommunication Terms 1.0

# 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.

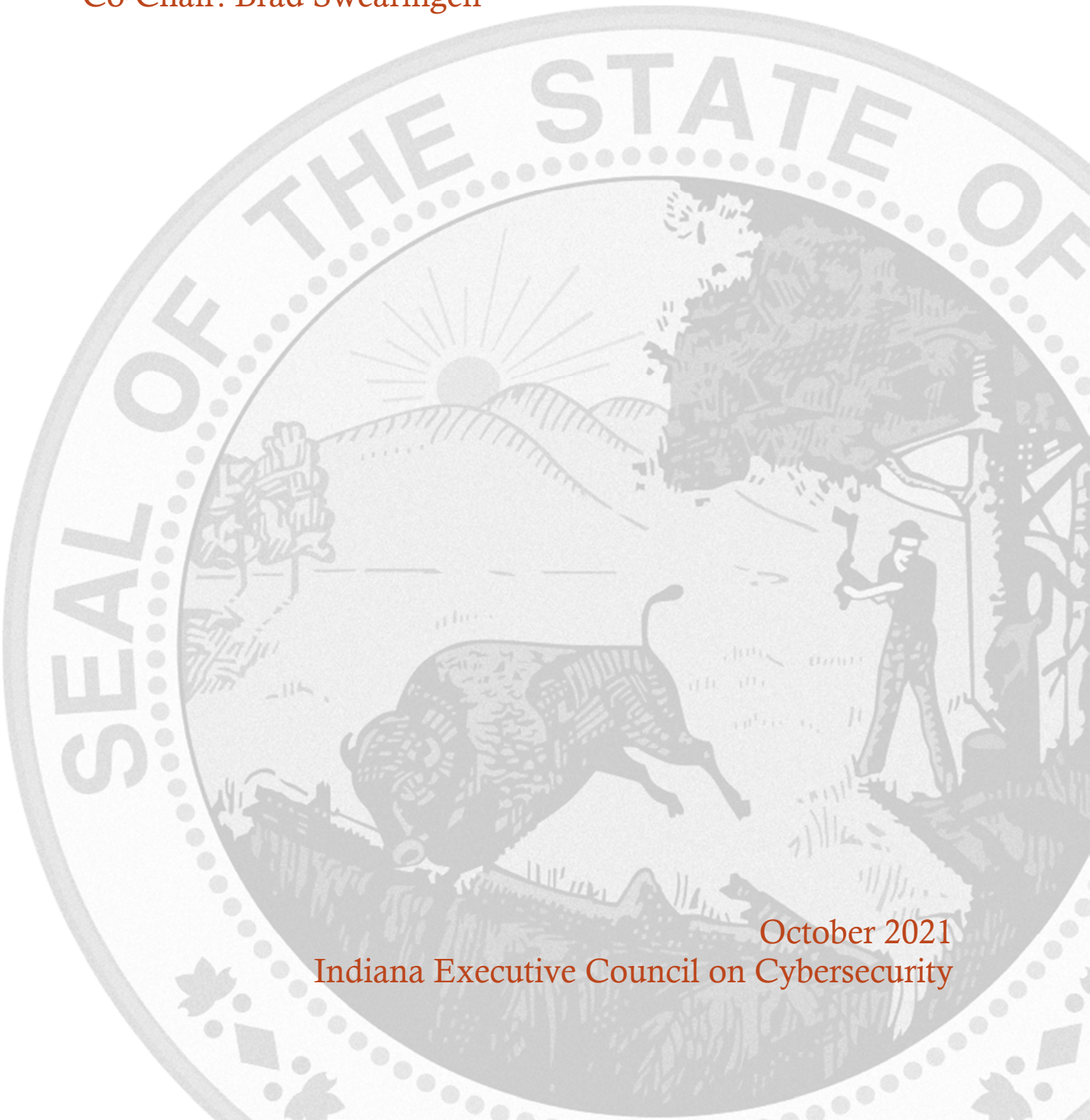
**5G**

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 Industrial Committee

# DEFENSE INDUSTRIAL COMMITTEE STRATEGIC PLAN

Chair: MG Clifton Tooley
Co-Chair: Brad Swearingen




October 2021
Indiana Executive Council on Cybersecurity

# Defense Industrial Committee Plan

# Table of Contents

# Committee Members

# Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Ehringer | David | Rolls Royce | Business Manager for IT Security | Full Time |
| Hormann | Douglas | Raytheon | Platform Systems / Cyber Lead | As Needed |
| Langley | Bryan | Indiana Economic Development Corporation | Senior Vice President of Defense | Chair Proxy |
| Reynolds | M. Brent | Naval Surface Warfare Center (NSWC) | Chief Scientist for Cybersecurity | As Needed |
| Silbaugh | Chris | Rolls Royce | Senior Security Strategy Officer | As Needed |
| Swearingen | Brad | Rolls Royce | Director of Cybersecurity, Defense Products | Co-Chair |
| Tooley | Cliff (GEN) | Indiana Economic Development Corporation | Director | Chair |
| Vespa | Tony | Vespa Group, LLC | Owner | Full Time |
| Werner | Kyle | Crane | Strategic Director | Full Time |
| Banta | Rich | Lifeline Datacenters | Principal & Chief Information Security Officer | Full Time |
| Chrislip | Chris | EICORP | Senior Cybersecurity Architect | As Needed |
| Jeffers | Chris | Indiana Economic Development Corporation | PTAC Director | Full Time |
| Ortiz | Jason | Pondurance | Senior Product Engineer | Full Time |
| Owen | Dan | Global Cyber Alliance | Domain Trust Product Owner | As Needed |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan.*

For more information, visit www.in.gov/cybersecurity.

# Executive Summary

# Executive Summary

- **Research Conducted**
  - The Defense Industry Committee leveraged a recently completed study of Indiana's defense market, with insights provided by 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.
    - Defense Reports (current standing in Defense programs)
    - Other states' Cybersecurity Defense Industry
    - Other states' 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 that 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
  - CMMC Training/Certification

- **Additional Notes:**
  - The Defense Industrial 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**

  - Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification - https://www.acq.osd.mil/cmmc/ (Dec. 2020)
  - U.S. Department of Defense – DoD to Require Cybersecurity Certification in Some Contract Bids https://www.defense.gov/News/News-Stories/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/
  - 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/
- Newman, Larry, *Shipley Proposal Guide for Business Development and Sales Professionals*, (Shipley Associates: 2009)
- 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 Under Secretary 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
- 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 more than 60% of small business fail within 6 months of a significant cyber incident such as a breach or ransomware. There is need for 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
    b. Working Digital platform
    c. Industry Lead Cyber Conference
    d. Defense Industry Legislative Recommendations
    e. 2% Market Share gain

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. A proactive, ongoing public awareness campaign consisting of key messages, delivered via social media and resources, tips and best practices is essential for educating and engaging people of all ages; a necessary element for providing the requisite protections needed for safeguarding our personal and financial information in all aspects of our everyday life.

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. 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 System

# Deliverable: Cyber Market System – Review

## *General Information*

1. **What is the deliverable?**
    a. Review of the 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?**
    ☒ Completed ☐ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

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. 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?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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

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. IEDC Defense Development

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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

## Tactic Timeline

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

## Resources and Budget (Please add rows as needed)

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

a. The Defense Committee will use current staff of IOT, IEDC, and other entities to complete this process.

**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?**

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. There is 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?**

☐No ☒ Yes

a. 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?**

☐No ☒ 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?**

☒No ☐ Yes

**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. Private and military partners.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

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

## Communications

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

a. IEDC Defense Development

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

☐No ☒ Yes

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

a. None

## *Evaluation Methodology*

**Objective 1:** IEDC Defense Development and partners will review the current cybersecurity market pursuit plan and system in 2021.

*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?**
    ☐ Completed ☐ In-progress 25% ☒ In-progress 50% ☐ In-progress 75% ☐ Not Started

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. 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?
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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

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. IEDC Defense Development

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**?

☐ One-time deliverable

☒ Ongoing/sustained effort

## Tactic Timeline (Please add rows as needed)

| **Tactic** | **Owner** | **% Complete** | **Deadline** | **Notes** |
|---|---|---|---|---|
| Minimum Viable Product Phase 1 | IEDC/NCCO | 100 | 2018 | This is a pilot. |
| Marketing Plan | IEDC/NCCO | 70 | 2021 | Unfunded |
| Training | IEDC/NCCO | 0 | 2021 | Unfunded |
| Support | IEDC/NCCO | 0 | 2021-2025 | Unfunded |

## Resources and Budget (Please add rows as needed)

**15. Will staff be required to complete this deliverable?**

☐No ☒ 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?**

| 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 are 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?**

☒No ☐ Yes

**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?**

☒No ☐ Yes

***Note:*** *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?**

☒No ☐ Yes

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

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

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

a. IEDC and National Center for Complex Operations (NCCO)

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. 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 IEDC Defense Development 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)?**

☐No ☒ Yes

a. 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:** IEDC Defense Development and partners will develop a pilot of the Indiana defense cybersecurity market development and capture plan and system (Digital Platform) by 2021.

*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 2025.
*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?**
   ☐ Completed ☐ In-progress 25% ☒ In-progress 50% ☒ In-progress 75% ☐ Not Started

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. 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?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☒ 2025+

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

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. IEDC Defense Development 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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Multi-Threat Energy Grid (M-TEG) | IEDC/NCCO | 100 | June 2020 | |
| Muscatatuck Cybertropolis (MUTC-C) | Indiana Guard | 100 | June 2020 | |
| Indiana Cyber Ecosystem (ICE) | IEDC/NCCO | 100 | June 2020 | |
| Capture market share statistics | IEDC | 20 | Ongoing until 2025 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| 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?**

| 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?**

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?**

☐No ☐ Yes

**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?**

☒No ☐ Yes

## 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?**

☒No ☐ Yes

**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. NCCO, IEDC, state and national stakeholders.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. 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. IEDC Defense Development

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

☐No ☒ 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:** IEDC Defense Development will establish a nationally recognized cybersecurity test bed in Indiana by June 2021.

*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 2025.

*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 Maturity Model Certification (CMMC) Compliant Program

# Deliverable: Cybersecurity Maturity Model Certification (CMMC) Compliant Program

## *General Information*

1. **What is the deliverable?**
   a. The Indiana Economic Development Corporation (PTAC/ ISBDC/Defense) and Purdue University (MEP/cyberTAP) are forming a partnership to support Indiana small businesses becoming level 1 Cybersecurity Maturity Model Certification (CMMC) Compliant.

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?**
   ☐ 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. Deliver CMMC technical assistance services to walk companies through the process of implementing CMMC standards and moving toward certification.

6. **What metric or measurement will be used to define success?**
   a. Clients Assisted or spoken with: Level 1- 40-60 – stretch goal (Fully implementing CMMC L1 controls).

   *Note: depending on level of assistance needed, the level of companies assisted can fluctuate.*

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

   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Indiana small businesses

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. Not Applicable. State agencies are not directly involved with the CMMC process, except IEDC. DLA (DoD) manages the CMMC process. Any potential overlap may come from third party vendors or other federal agencies who may provide additional resources that could be applicable to CMMC (i.e., SBA).

## Additional Questions:

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Defense at this present 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. IEDC and Purdue University

12. **Who should be main lead of this deliverable?**
    a. Bryan Langley and Chris Jeffers

13. **What are the expected challenges to completing this deliverable?**
    a. Formulating a process that addressing a fluctuating defense program, with an increased demand and need for Indiana companies.

# *Implementation Plan*

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

    ☐ One-time deliverable

    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Process to manage support | IEDC/Purdue | 100 | Oct 2021 | Program is expected to be active in Dec. |

## Resources and Budget

**15. Will staff be required to complete this deliverable?** ☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| N/A | N/A | Existing staff | IEDC | | This process has been built in using existing funds |

**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 |
|---|---|---|---|---|---|---|
| Purdue | Already built in | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Support Indiana small businesses becoming level 1 Cybersecurity Maturity Model Compliant (CMMC)

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

a. It is based on CMMC compliance that includes a cost that will be incumbered on businesses. The support we are providing helps them move to L1 certification, so the cost and support is more around getting companies equipped.

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

a. Indiana companies not being CMMC compliant and losing defense contracts.

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

a. Based on how many companies we can support through the process. 40-60 companies.

**21. 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

**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?**

☐No ☒ Yes

a. The partnership between IEDC and Purdue is unique among most states because we are leveraging available resources to support companies.

## 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?**

☒No ☐ Yes

a. If yes, what is the change and what could be the fiscal impact if the change is made? No – however additional support from the state will help us increase the resources available to companies, although the cost of being CMMC compliant falls primarily on the company

**25. What will it take to support this deliverable if it requires ongoing sustainability? Federal and state funding.**

a. Both

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

a. IEDC and Purdue customers and vendors

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes,

a. Any committee that works with businesses and eventually, government sectors

## Communications

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

a. Indiana small businesses and IEDC stakeholder groups, to include the IECC. Purdue will also provide information to their clients and customers.

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

☐No ☒ Yes

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

a. No Response

## *Evaluation Methodology*

**Objective 1:** IEDC and partners will develop a Cybersecurity Capability Maturity Model (CMMC) framework in Indiana by December 2021.

*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:** IEDC and partners will promote Cybersecurity Capability Maturity Model (CMMC) in Indiana to 80% of key stakeholders and associations by January 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

# Supporting Documentation

# Supporting Documentation

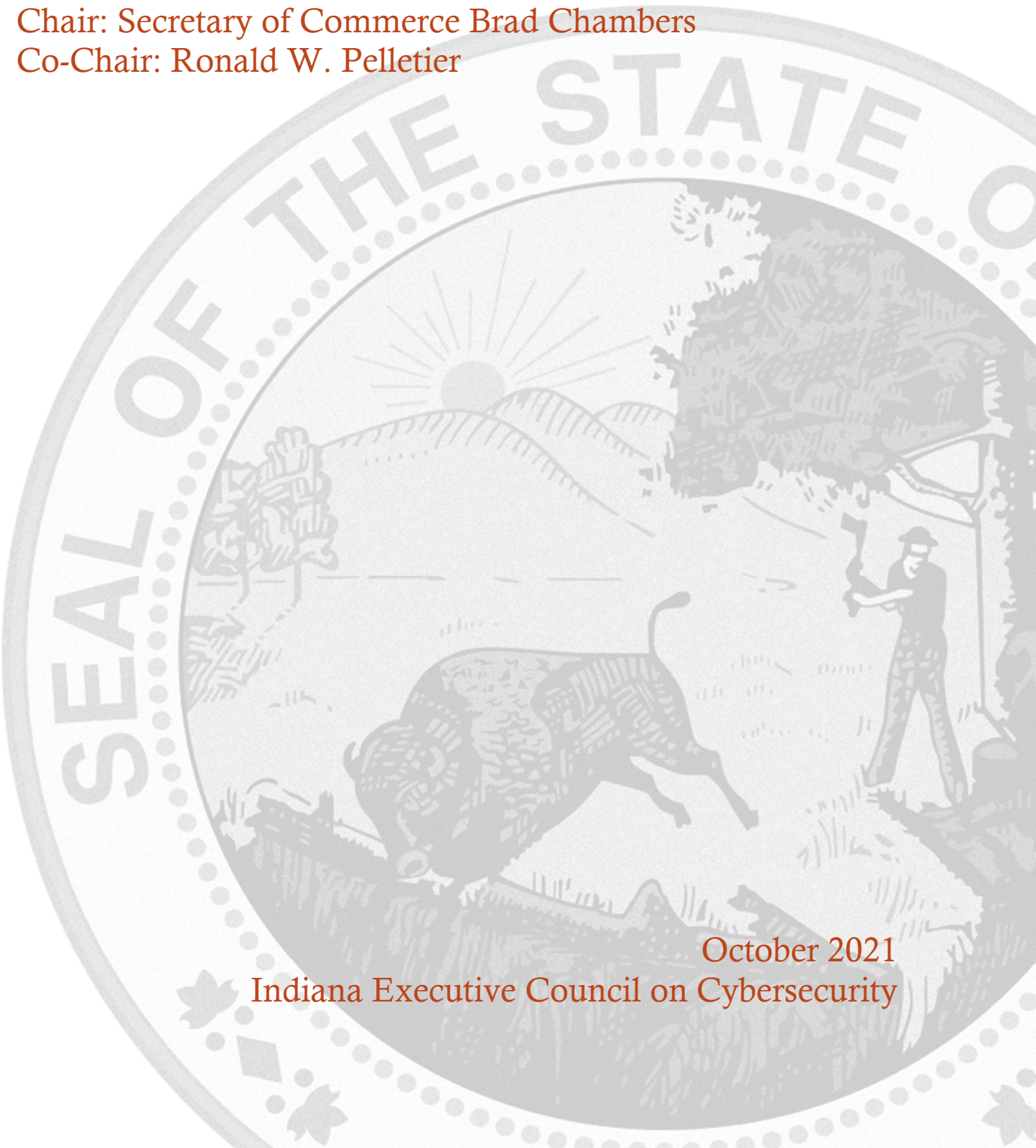
This section contains all the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

There are no supporting documents at this time


# Appendix D.3
## Economic Development Committee

# ECONOMIC DEVELOPMENT COMMITTEE STRATEGIC PLAN

Chair: Secretary of Commerce Brad Chambers
Co-Chair: Ronald W. Pelletier



October 2021
Indiana Executive Council on Cybersecurity

# Economic Development Committee Plan

# Table of Contents

# Committee Members

# Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Jeffers | Chris | Indiana Economic Development Corporation | PTAC Director | Full Time |
| Lubbers | Teresa | Indiana Commission for Higher Education | Commissioner | Full Time |
| Ortiz | Jason | Pondurance | Senior. Product Engineer | Full Time |
| Pelletier | Ronald W. | Pondurance | Founding Partner | Co-Chair |
| Rapp | Douglas | Cyber Leadership Alliance | President | Full Time |
| Roberts | David | Indiana Economic Development Corporation | Vice President, Chief Innovation Officer, Business Development | Chair Proxy |
| Staton | Jim | Indiana Economic Development Corporation | Senior Vice President and Chief Business Development Officer | Full Time |
| Thompson | JJ | Alpine Start | Founder | As Needed |
| Wasky | Mark | Indiana Economic Development Corporation | Vice President & Counsel, Government & Community Affairs | As Needed |
| Watkins | David | Indiana Economic Development Corporation | SBDC State Director | Full Time |
| Silbaugh | Chris | Rolls Royce | Senior Security Strategy Officer | Full Time |

| | | | | |
|---|---|---|---|---|
| Chambers | Brad | Indiana Economic Development Corporation | Secretary of Commerce | Chair |
| Langley | Bryan | Indiana Economic Development Corporation | Senior Vice President of Defense | Full Time |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan.*

For more information, visit www.in.gov/cybersecurity.

# 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 report commissioned by the Indiana Economic Development Corporation (IEDC), comparisons with other state's indicated initiatives (e.g., GA, MI, MD, KY, LA, CO, etc.), employment data reported by US Department of Labor, Office of Economic Adjustment, and Emsi Occupation Snapshot Report for Q4 2017 (central Indiana).
    - 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.

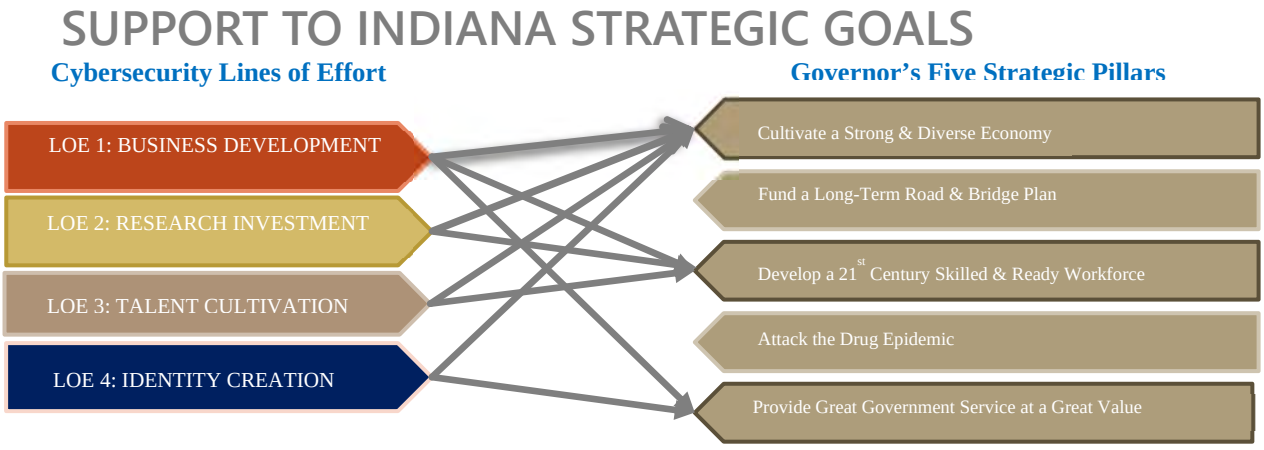
- **Research Findings**
  - Our review of the economic development strengths, weaknesses, opportunities, and threats (SWOT) of cybersecurity led the group to the following conclusions:
    - Cybersecurity should not be thought of as a discrete sector. Rather, all companies must have a cybersecurity awareness and plan in order to win and, in some cases, to even compete for business opportunities.
    - Cybersecurity is one of the fastest growing areas within the technology sector. Based on data from the U.S. Bureau of Labor Statistics' Information Security Analyst's Outlook, cybersecurity jobs are among the fastest-growing career areas nationally. The BLS predicts cybersecurity jobs will grow 31% through 2029; a rate that is over seven times faster than the national average job growth of 4%.
    - Cybersecurity Ventures predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the five-year period from 2017 to 2021.
    - Cybersecurity The global cybersecurity market size is forecast to grow to $345.4 billion U.S. dollars by 2026.
    - Indiana's largest assets are Academia and Innovation and Entrepreneurship (per IEDC report found in supporting documentation section).
    - 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 points , one important finding during the working group's research showed that Hoosiers believe the most important role of government in cybersecurity business development is positive economic climate, strategic leadership, and business incentives.

- **2021 Committee Deliverables**
  - Incentive Program
  - Cyber Business Attraction Package
  - Cybersecurity Maturity Model Certification (CMMC) Outreach Plan

- **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 Report 2017
  - Mlitz, Kimberly, Cybersecurity Market Revenues Worldwide, 2021-2026
  - Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021 - https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem
  - Morgan, Steve, http://cybersecurityventures.com/cybersecurity-market-report/
  - "Cyber Threat: Indiana's Call to Action," Anita Nerses (Raytheon), Inside Indiana Business, August 9, 2017. 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.
  - 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.
  - Emsi Occupational Snapshot Report, Q4 2017. www.economicmodeling.com

# 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 (K-12 computer skills 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. International Securities Services Association (ISSA) and Indiana Systems Audit and Control Association (ISACA) chapters remain active as well as Infragard
   f. K-12 requirements as part of Next Level agenda
   g. Indiana Information Sharing and Analysis Center (IN-ISAC)

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. General Data Protection Regulation (GDPR) based on 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. Baltimore, Maryland, 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. Cyber California

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 Initiatives
   b. Cyberpoint Technology & Innovation Center proposal to City of Baltimore
   c. "Uncharted: New Partners Team up as Georgia Stakes its Claim on Cyber Leadership," 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 the 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 K-12 and track talent
   e. Identify current assets and capabilities better (e.g., INFRAGARD, Henry St. DHS)
   f. Publicize this Council and their efforts
   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-focused companies
b. Cyber-focused companies with office in Indiana
c. Companies that do cyber but not as their primary focus
d. Cybersecurity workforce using the updated tools from DWD using CyberSeek.org

**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 and/or 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 and control of battery and gen-sets for critical infrastructure)

c. Recommended incentives for consideration:
   - 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)
   - 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 percent, up to $1 million.

**12. What are your communication protocols in a cyber emergency?**
Not applicable.

**13. What best practices should be used across the sectors in Indiana?**

a. Use NIST standards for definitions
b. Increase awareness and messaging of threat and opportunity

# Deliverable: Investment

# Deliverable: Investment

## *General Information*

1. **What is the deliverable?**
   a. Develop a framework of potential economic development support for Indiana businesses seeking to improve their cybersecurity posture and thrive in the federal cybersecurity environment.

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.**
   a. Strengthen best practices to protect information technology infrastructure.
   ☐ 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. It is the goal of this working group deliverable to develop an economic development framework that supports investment in Indiana businesses engaging in the cybersecurity landscape. The resulting action or modified behavior of this deliverable would be the improved cybersecurity posture and success of Hoosier businesses.

6. **What metric or measurement will be used to define success?**
   a. Success will be defined by the deployment of an economic development framework that the IEDC can use to invest in new companies that begin in, or move to, Indiana as well as those existing Indiana companies seeking to improve their cybersecurity preparedness.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☐ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Indiana businesses and businesses considering starting or locating in Indiana

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. Defense Industrial Committee, Cyber Awareness and Sharing Working Group, Workforce 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. IEDC

12. **Who should be main lead of this deliverable?**
    a. IEDC Chief Innovation Officer

13. **What are the expected challenges to completing this deliverable?**
    a. Funding and legislative priorities

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Research market needs around cybersecurity | IEDC | 0% | June 2022 | |

| | | | | |
|---|---|---|---|---|
| Research other successful business investment and support programs | Economic Development committee | 0% | June 2022 | |
| Meet with IEDC executive team | Economic Development committee | 0% | December2022 | |
| Put together framework recommendation | Economic Development committee | 0% | January 2023 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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 initiative will encourage cybersecurity investments in the state of Indiana by companies looking to start, grow, or relocate in Indiana.

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

a. By developing a framework for economic development support of businesses in relation to cybersecurity, the cybersecurity of the entire State will be enhanced and business resiliency improved.

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

a. By not developing a framework for economic development support and investment in improvements in the cybersecurity posture of Indiana businesses, the State risks a scattered and uncoordinated approach to cybersecurity development and support.

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

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. The baseline should be reflective of today's business environment

**21. 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

**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?**

☐No ☒ Yes

a. 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
b. The desire of this subcommittee to not require audits and rely on self-reporting which may not prove to be reliable
c. Not enough funding to support future investments

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

☐No ☒ Yes

a. Regulation and policy may be required to create and enable potential new support framework.

**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?**

☐No ☒ Yes

a. There could be potential overlap with the Workforce Development Committee and Defense committee.

## 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)?**

☐No ☒ Yes

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

a. No response.

## *Evaluation Methodology*

**Objective 1:** The Economic Development Committee with the IEDC will develop an economic development support framework for Indiana companies to thrive in the cybersecurity landscape by December 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

**Objective 2:** Companies that move, start, or grow here will have a framework for economic development support 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

# Deliverable: Leadership

# Deliverable: Leadership

## *General Information*

**1. What is the deliverable?**

Leverage and raise awareness of the resources available from Indiana academic institutions, defense assets, private sector, and governmental entities to promote Indiana's thought leadership in innovation and cybersecurity.

**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?**

☐ 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. Highlight and support the research and capabilities of Indiana defense assets, private sector partners, governmental entities, and universities such as Purdue, IU, Notre Dame, Rose Hulman, Butler, Ivy Tech, etc. as it relates to cybersecurity to position Indiana as a thought leader on the national stage.
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 public-private partners, out-of-state cybersecurity influencers, and governmental entities.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☐ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. New and existing businesses, Indiana universities, and Hoosiers across the State would benefit from a position as a cybersecurity thought leader and convener of discussions around cybersecurity research, innovation, and technology.
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. Cyber Awareness and Sharing 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. Defense development, Homeland security, DOD, Department of Commerce, SBA and others all have a role to play in cybersecurity leadership and awareness building.

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

13. **What are the expected challenges to completing this deliverable?**
    a. Many states and cities are competing in this area. Standing out of the crowd will be difficult for a non-traditional cybersecurity locale such as Indiana.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Generate list of highlights and support activities | ED Subcommittee | 10% | December 2022 | |
| Lend IEDC backing/support to select initiatives & activities | ED Subcommittee | 10% | December 2023 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1 | N/A | IEDC | State | N/A | Existing staff that interact with cybersecurity activities |

**16. What other resources are required to complete this deliverable?**

a. No response

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Greater awareness of Indiana's position as a thought leader on cybersecurity issues.

**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. Indiana could be passed by other States seeking to establish a reputation as cybersecurity focused.

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

a. Greater awareness of cybersecurity thought leadership and activities – number of support initiatives tied to cybersecurity.

**21. 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

**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?**

☐No ☒ Yes

## 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?**

☒No ☐ Yes

**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. Indiana academic institutions, private sector partners, and governmental entities.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

## 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)?**

☐No ☒ Yes

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

a. This list should emphasize cyber-related events and updates

## *Evaluation Methodology*

**Objective 1:** Indiana Economic Development Corporation and Committee will work to identify potential partners, activities, and initiatives of cybersecurity influencers in the State of Indiana by December 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

**Objective 2:** Measure the effectiveness of IEDC supported activities and initiatives in the cybersecurity space 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

# Deliverable: Technical Assistance

# Deliverable: Technical Assistance

## *General Information*

1. **What is the deliverable?**
   a. Address the growing need for small businesses to deploy cybersecurity best practices by delivering technical assistance programming and services through the IEDC and its partners.

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?**
   ☐ 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. Develop a plan for the implementation of technical assistance programs that will assist small businesses with cybersecurity awareness and outreach, assessment tools, training opportunities, and direct support with CMMC Level 1 implementation.

6. **What metric or measurement will be used to define success?**
   a. Clients Assisted or spoken with  Level 1- 40-60 – stretch goal (Fully implementing CMMC L1 controls).

   *Note: depending on level of assistance needed, the level of companies assisted can fluctuate.*

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

   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Indiana small businesses

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. DLA (DoD) manages the CMMC process.  Any potential overlap may come from third party vendors or other federal agencies who may provide additional resources that could be applicable to CMMC (i.e., MEP, SBA).

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Defense Industrial Committee and Cyber Awareness and Sharing 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. IEDC and Purdue University

12. **Who should be main lead of this deliverable?**
    a. IEDC: Bryan Langley and Chris Jeffers

13. **What are the expected challenges to completing this deliverable?**
    a. Formulating an outreach plan that will adequately addresses a fluctuating training program, with an increased demand and need for Indiana companies, primarily in the area of defense companies.

## *Implementation Plan*

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

    ☐ One-time deliverable

    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Process to manage support | IEDC/Purdue | 100 | October 2021 | Program is expected to be active in Dec. |
| Develop outreach plan | IEDC | 50% | January 2022 | |
| Implement outreach plan | IEDC with partners | 10% | February 2022 | |
| Evaluate effectiveness of outreach plan | IEDC | 0% | February 2023 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| No Response | No Response | Existing staff | IEDC | | This process has been built in using existing funds |

**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 |
|---|---|---|---|---|---|---|
| Purdue | Already built in | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Support Indiana small businesses to implement cybersecurity best practices such as becoming Level One(L1) Cybersecurity Maturity Model Compliant (CMMC)

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

a. Will involve having more Indiana small businesses trained and aware of cybersecurity best practices, thereby reducing cybersecurity risk. Based on CMMC compliance, that includes a cost that would normally be charged to the businesses. The support we are providing helps them move to L1 certification, so the cost and support is more around getting companies equipped.

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

a. Indiana companies not being CMMC compliant and losing defense contracts.

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

a. Based on how many companies we can support through the process, 40-60 companies.

**21. 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

**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?**

☐No ☒ Yes

## 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?**

☒No ☐ Yes

a. No, however additional support from the state will help us increase the resources available to companies, although the cost of being cybersecurity prepared falls primarily on the company.

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

a. Both federal and state funding.

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

a. Indiana small businesses, the IEDC and Purdue customers and vendors

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. Any committee that works with businesses and eventually, government sectors

## Communications

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

a. Indiana small businesses and IEDC stakeholder groups, to include the IECC. Purdue will also provide information to their clients and customers.

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

☐No ☒ Yes

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

a. Any training program, while primarily for companies who serve the defense industry, could be suitable for all types of industries. So, the reach of the program may be larger than anticipated.

b. The partnership between IEDC and Purdue is unique among most states because we are leveraging available resources to support companies.

## *Evaluation Methodology*

**Objective 1:** IEDC and partners will develop a cybersecurity technical assistance plan in Indiana by January 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

**Objective 2:** Measure the effectiveness of the Cybersecurity technical assistance plan by the number of participants (40) by February2023.

*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 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

# IECC Economic Development Corporation
# Cyber Initiative Report

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.

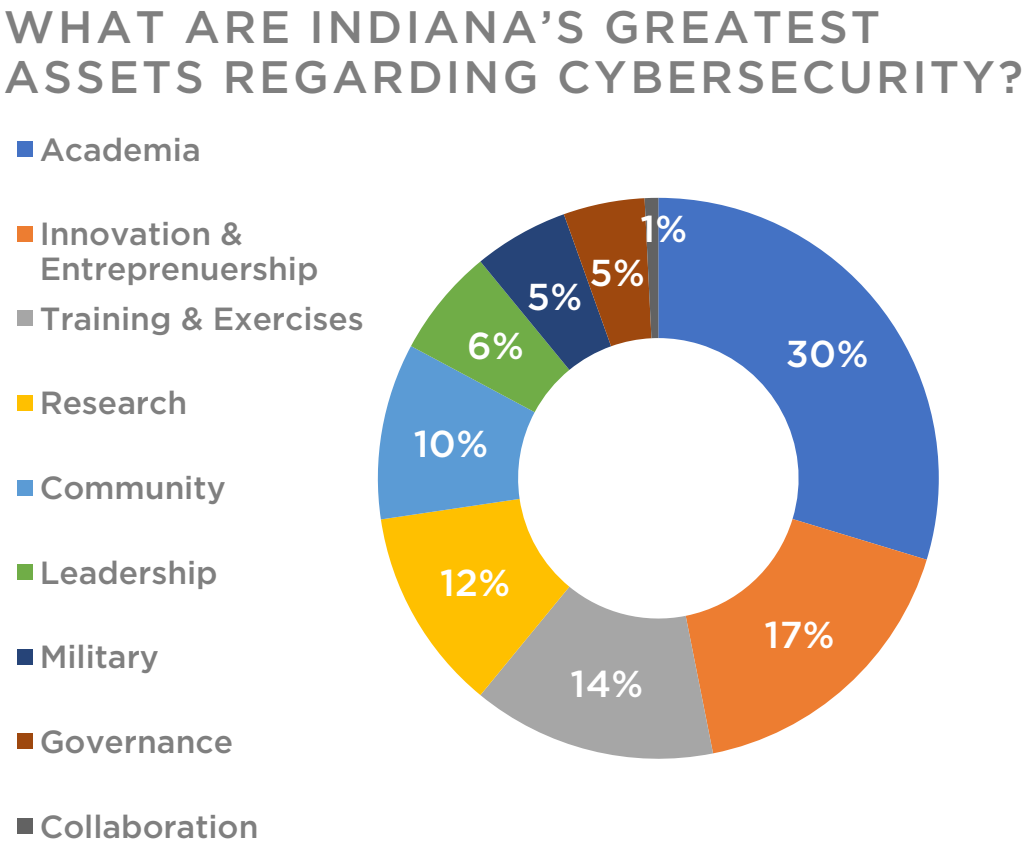



*Figure 1. Indiana cybersecurity industry survey results on greatest assets.*

[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.

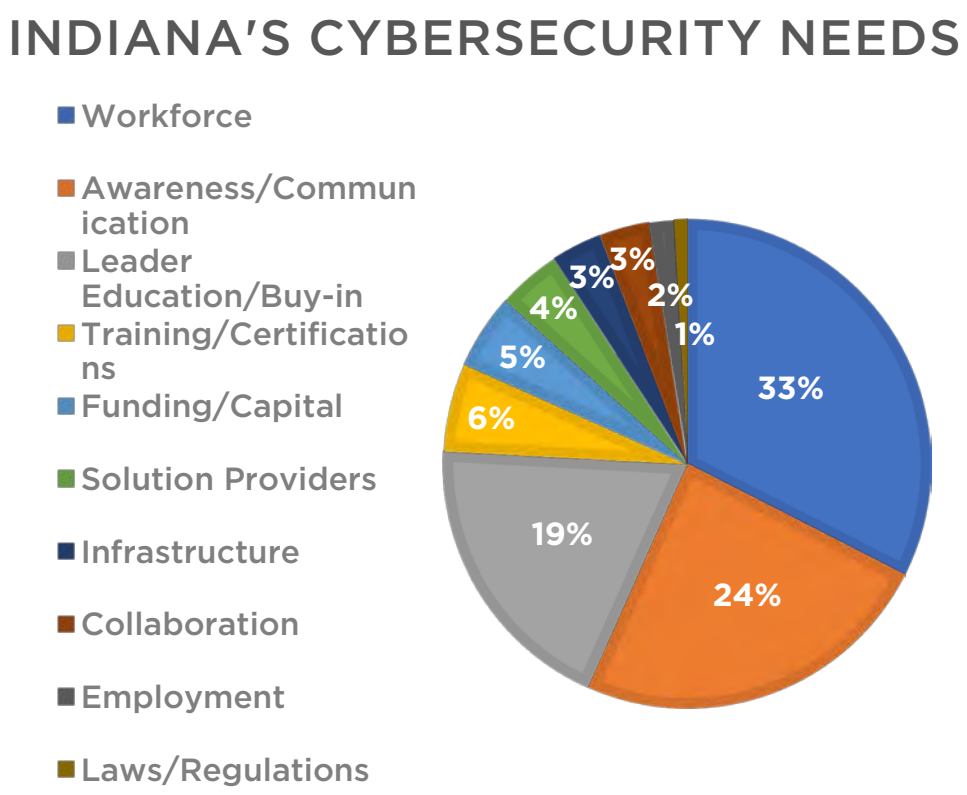



*Figure 2. Indiana cybersecurity industry survey results on greatest cybersecurity needs.*

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.

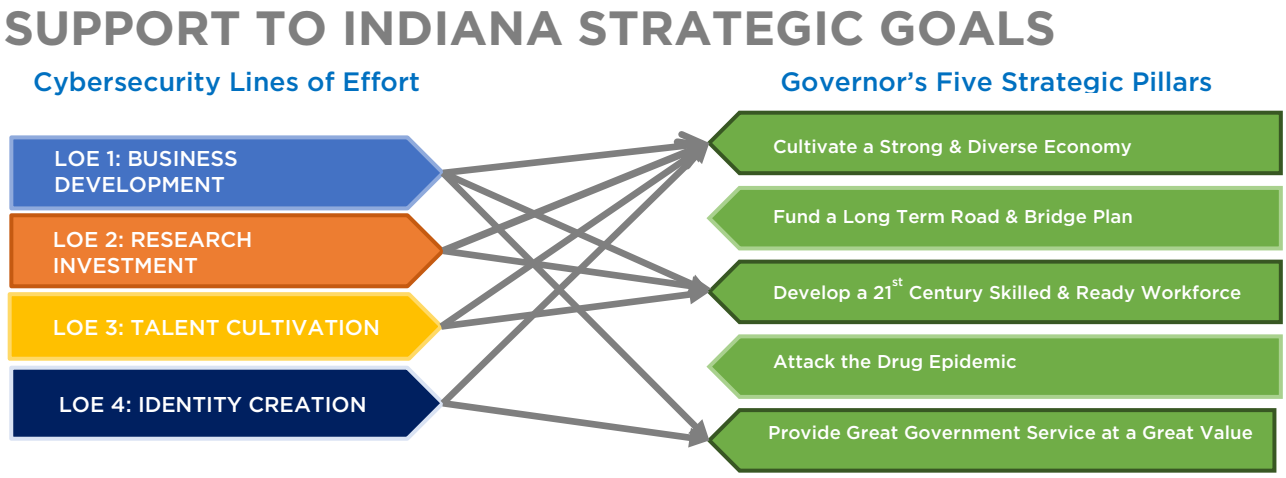



Figure 4. Cybersecurity lines of effort support to Indiana Strategic Goals

## 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.

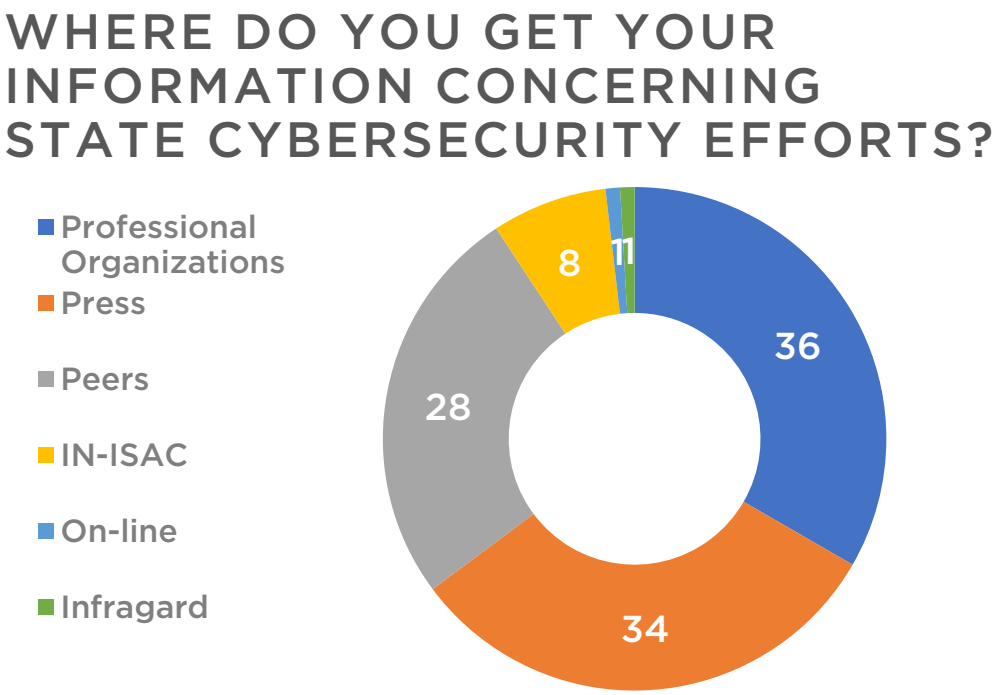



*Figure 5. Indiana cybersecurity industry survey results on State information.*

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.

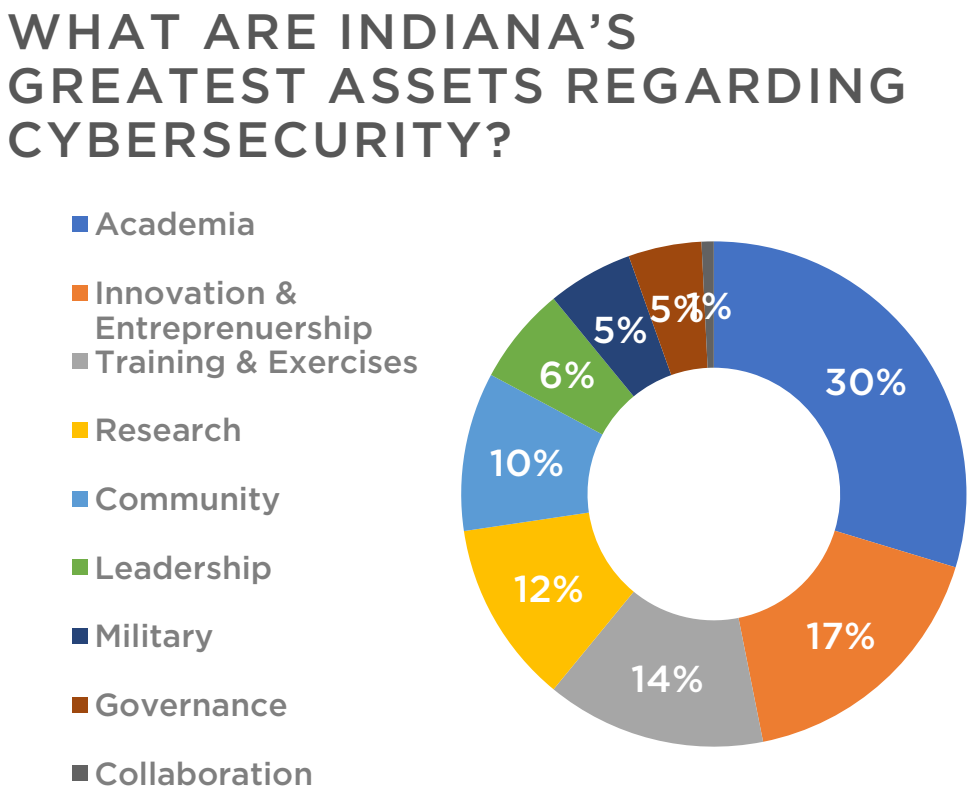
Current Executive Orders can be found at http://www.in.gov/gov/2384.htm.

### Annex B: Indiana Economic Development Corporation Cybersecurity Survey

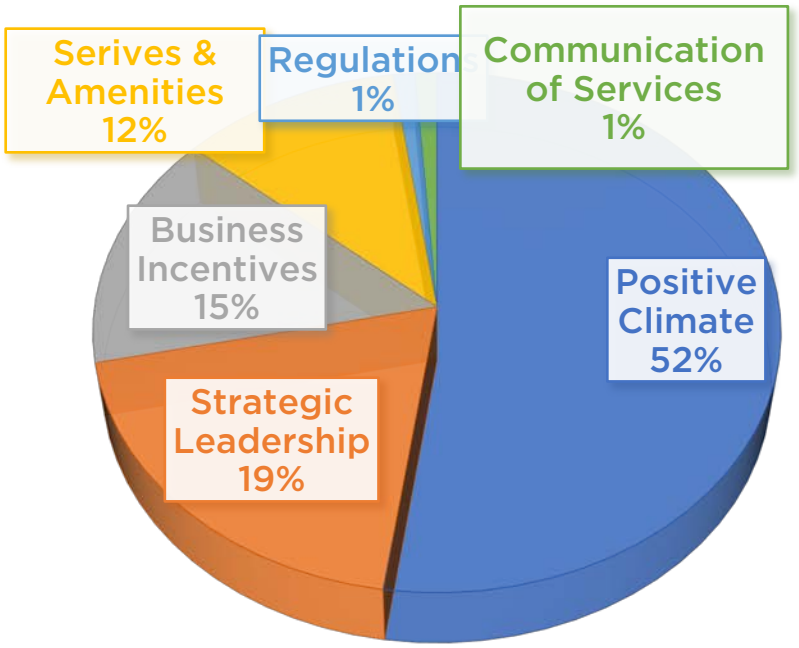
The IEDC developed and conducted a cybersecurity industry survey which was distributed in hard copy to participants of the Cybersecurity Town Halls as well as made available online. The purpose of the survey was to

- 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

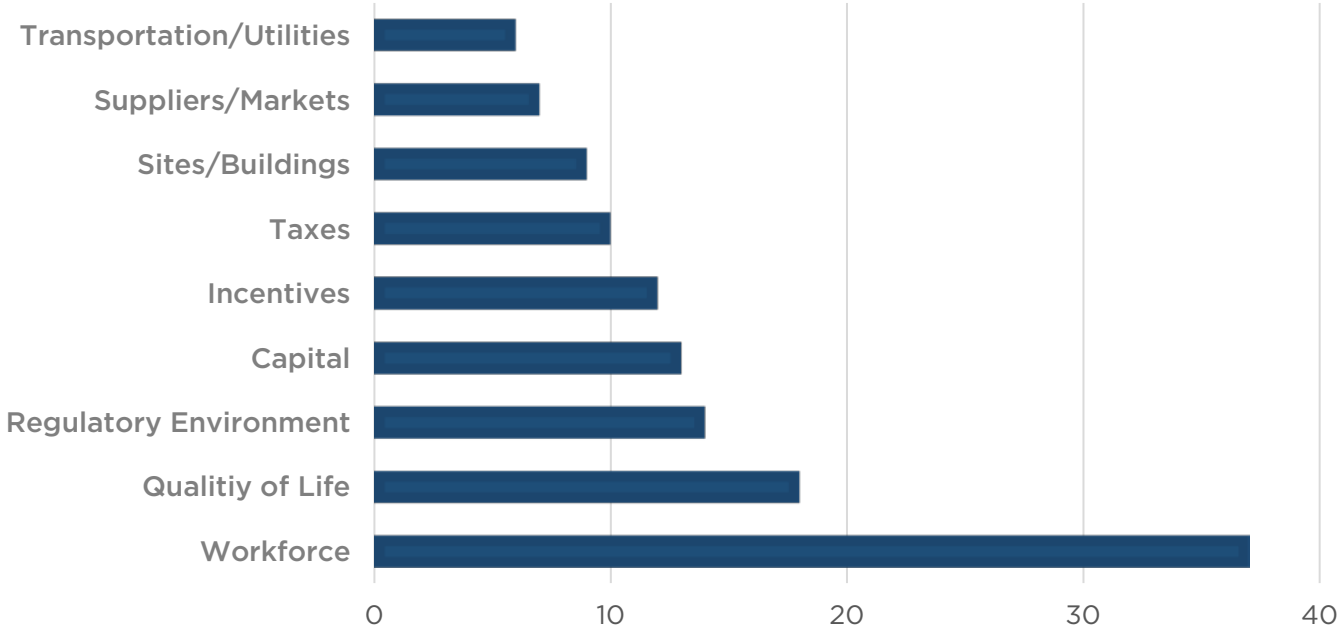
Highlights of the survey results that were key to the development of this plan are depicted below.



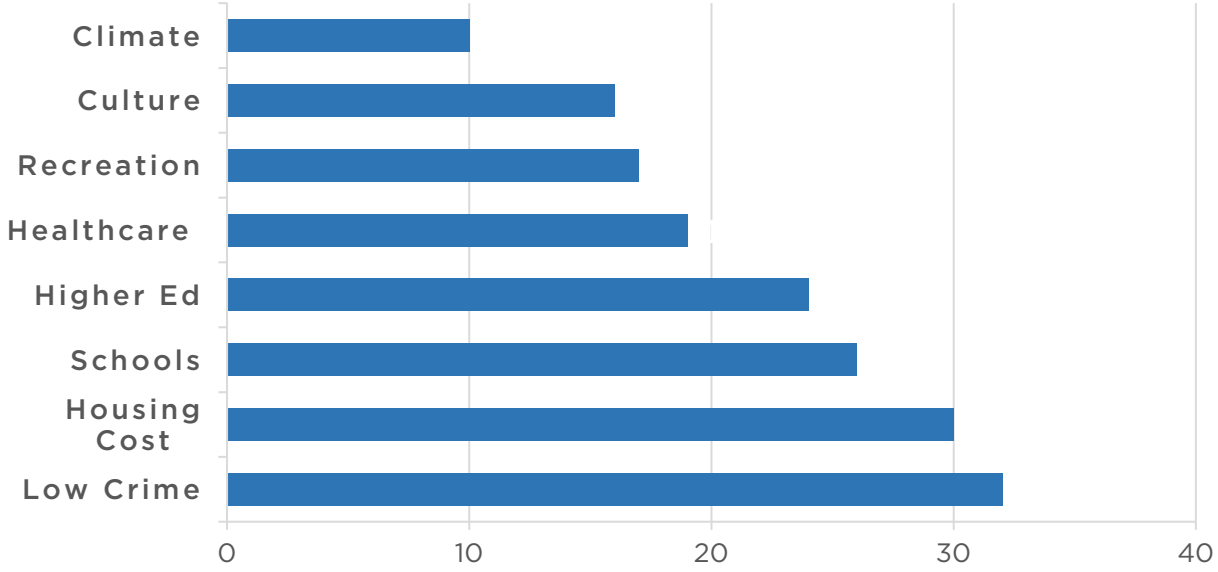
# WHAT IS THE MOST IMPORTANT ROLE OF GOVERNMENT IN BUSINESS DEVELOPMENT?




# 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.<br>• An innovation and entrepreneur community that could benefit from economic gardening.<br>• 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.<br>• A need for local cybersecurity certification training.<br>• A desire to leverage military assets.<br>• A Shortage of workforce.<br>• A need for small and mid-size business cybersecurity solutions. |
| Evansville | • A desire for better communication within the state on cybersecurity information and initiatives.<br>• A high concentration of expertise within utilities (energy).<br>• A high concentration of cybersecurity expertise and need surrounding advance manufacturing and industrial control systems.<br>• A need for small and mid-size business cybersecurity solutions.<br>• A shortage of workforce. |
| Fort Wayne | • A need and desire to develop regional cybersecurity strategies.<br>• A high concentration of expertise in health care, medical devices and advanced manufacturing.<br>• A need for small and mid-size business cybersecurity solutions.<br>• A shortage of workforce. |

| | |
|---|---|
| Portage | • A need for small and mid-size business cybersecurity solutions.<br>• A need and desire to develop regional cybersecurity strategies.<br>• A desire to leverage military assets.<br>• A shortage of workforce. |
| Westgate | • A desire to leverage military assets.<br>• Many assets and individuals that could be more effectively engaged by the State.<br>• A need for investment in infrastructure.<br>• A shortage of workforce. |
| West Lafayette | • Many assets and individuals that could be more effectively engaged by the State.<br>• Opportunities to unlock intellectual property from higher education.<br>• An innovation and entrepreneur community that could benefit from economic gardening. |

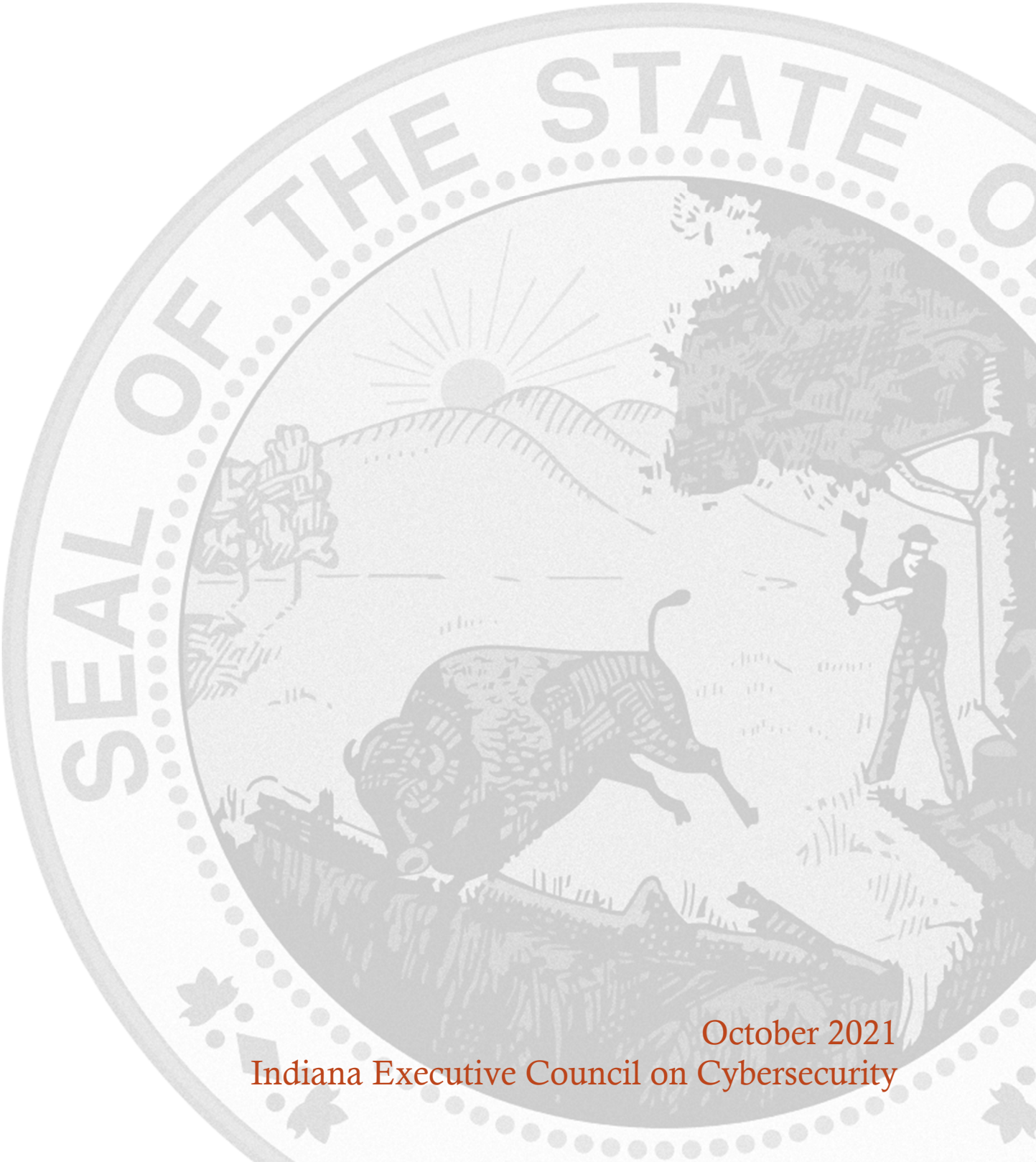
## Annex D: Indiana Cybersecurity Engagement Activities

| 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 Holli Sullivan
Co-Chair: Beth Dlug




October 2021
Indiana Executive Council on Cybersecurity

# Election Committee Plan

# Table of Contents

# Committee Members

# Committee Members

| Last Name | First Name | Organization | Organization Title | Member Type |
|---|---|---|---|---|
| Bagga | Jay | Ball State University VSTOP | Co-Director, State of Indiana Voting Systems Technical Oversight Program (VSTOP), Professor of Computer Science | Full Time |
| Bailey | Gerry | Corvano LLC | President | As Needed |
| Bonnet | Jerry | Indiana Secretary of State | General Counsel | As Needed |
| Byers | Bryan | Ball State University VSTOP | Co-Director, State of Indiana Voting Systems Technical Oversight Program (VSTOP), Professor of Criminal Justice and Criminology | As Needed |
| Cooper | Seth | Baker Tilly | Project Manager | As Needed |
| Dlug | Beth | Allen County Election Board | Elections Director | Co-Chair |
| Fahey | Sean | CIVIX (PCC) | Elections and Campaigns | As Needed |
| Frank | Michael | Anderson University | Professor of Political Science | As Needed |
| Herzog | Laura | Hendricks County | Elections Supervisor | Full Time |
| Hoffmeyer | Rachel | Indiana Secretary of State | Deputy Secretary of State | Full Time<br>Chair Designee-Proxy |
| King | Brad | Indiana Election Division | Election Division Co-Director | Full Time |
| Kochevar | Matthew | Indiana Election Division | Co-General Counsel | As Needed |

| | | | | |
|---|---|---|---|---|
| Mays | Lindsey | Indiana Secretary of State | IT Director | As Needed |
| Nussmeyer | Angela | Indiana Election Division | Election Division Co-Director | Full Time |
| Sullivan | Holli | Indiana Secretary of State | Secretary of State | Chair |
| Welch | Von | Indiana University | Associate Vice President for Information Security | As Needed |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

# 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 (Revised July 2021)**
  - **Collaboration with Federal and Sector Communities of Interest**
    Since the heightened concern over election interference in 2016 and federal designation of Elections as Critical Infrastructure in 2017, communities of interest have come together to provide a significant level of resources focused on election security. The Secretary of State may engage in election cybersecurity collaboration with the following allied organizations:
    - DHS, DOD, US Cyber Command
    - Center for Internet Security
    - Election Infrastructure Information Sharing and Analysis Center
    - MS-Election -ISAC
    - Cybersecurity and Infrastructure Security Agency Election Security Initiative

[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.

- National Association of Secretaries of State
- National Association of State Election Directors
- U. S. Election Assistance Commission (EAC)
- Indiana Fusion Center
- Indiana Executive Council on Cybersecurity
- Association of the Clerks of the Circuit Courts of Indiana
- Indiana Statewide Voter Registration System Core Team
- Indiana Voting System Technical Oversight Program (VSTOP)
- Indiana Voter Registration Association
- EAC accredited Voting System Testing Labs (VSTLs)
- Association of Government IT Leaders (GMIS.org)

- **Integration of Cybersecurity Professionalism, Awareness and Practice**
  - The Secretary of State will promote integration of experienced, trained, and professionally certified cybersecurity resources into all phases of election administration.
  - State and local election officials and administrators will be encouraged to engage Certified Information Security Professionals, and provide ongoing cybersecurity awareness, training, and certification opportunities for staff.
  - The Secretary of State will assist VSTOP with the integration of election cybersecurity into the Election Administration Certificate Program (CEATS).

- **Election Infrastructure Monitoring, Hardening, Testing and Auditing**
  The Secretary of State will promote election infrastructure cyber security monitoring and improvements in the following aspects:
  - Monitoring with the use of state-of-the-art contractors and protocols
  - Hardening via technical and process improvements
  - Voting system and electronic poll book testing and certification protocols, and implementation of paper audit trail voting systems
  - Post-election risk-limiting audit program development, funding, and implementation

- **Public Engagement and Confidence**
  The Secretary of State will maintain a high level of public engagement in the area of election security and public confidence including:
  - Surveying the public about election security and integrity concerns
  - Voter outreach, education, and engagement activities
  - Implementation of absentee voting Internet enabled and assistive technology for blind and print disabled voters

- **Continuity, Coordination, Maintenance of Effort and Oversight**
  To assure the highest level of ongoing election cybersecurity vigilance and effort, the Secretary of State may integrate the IECC Election Committee's day-to-day, and election-to-election responsibilities with the professionally managed Indiana Statewide Voter Registration System Core Team.

• **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 continues 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.

- The Secretary of State and Indiana Election Division have been engaged administering Help America Vote Act (HAVA) Election Security Fund appropriated by Congress in 2018 and 2020 ($16,140,537 for Indiana) and $10,000,000 appropriated by the Indiana General Assembly for election cybersecurity initiatives.
  The 2018 – 2022 Election security initiatives include:

  a) grants to counties for to improve physical security of election equipment
  b) grants to counties to upgrade voting equipment (to include voter verifiable paper trails)
  c) implementation of county level and Statewide Voter Registration System network security monitoring
  d) electronic pollbook hardware and software upgrades
  e) network penetration testing exercises
  f) conducting post-election Risk Limiting Audits to confirm election outcomes.

# 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 cyber threats. 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).
o. Grants to counties for to improve physical security of election equipment.
p. Grants to counties to upgrade voting equipment (to include voter verifiable paper trails).
q. Implementation of county level and Statewide Voter Registration System network security monitoring
r. Electronic poll book hardware and software upgrades.
s. Network penetration testing exercises.
t. Conducting post-election Risk Limiting Audits to confirm election outcomes.

**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 sophisticated domestic or overseas perpetrators.
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 (IoT) 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.**
    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
    b. Year Three- deliverables developed with training programs
    c. Year Five – no successful penetration of election systems or databases essential to conducting elections; overall high level of public confidence in election security and outcomes.

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 inform the public promptly and accurately 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 was developed and launched in time for the November 2018 General Election.
    c. VSTOP 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 administering an election is to be immediately reported to the Secretary of State.
    b. The Secretary of State will communicate the details of the incident to appropriate responding security, 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?**

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: Collaboration with State, Federal, and Sector Communities

# Deliverable: Collaboration with State, Federal, and Sector Communities

## *General information*

1. **What is the deliverable?**
   a. Collaboration with State, Federal and Sector Communities
      - Since the heightened concern over election interference in 2016 and federal designation of Elections as Critical Infrastructure in 2017, communities of interest have come together to provide a significant level of resources focused on election security. The Secretary of State will continue engage in election cybersecurity collaboration with the following allied organizations:

        - DHS, DOD, US Cyber Command
        - Center for Internet Security
        - Election Infrastructure Information Sharing and Analysis Center
        - MS-Election -ISAC
        - Cybersecurity and Infrastructure Security Agency Election Security Initiative
        - National Association of Secretaries of State
        - National Association of State Election Directors
        - U. S. Election Assistance Commission (EAC)
        - Indiana Fusion Center
        - Indiana Executive Council on Cybersecurity
        - Association of the Clerks of the Circuit Courts of Indiana
        - Indiana Statewide Voter Registration System Core Team
        - Indiana Voting System Technical Oversight Program (VSTOP)
        - Indiana Voter Registration Association
        - EAC accredited Voting System Testing Labs (VSTLs)
        - Association of Government IT Leaders (GMIS.org)

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?**
   ☐ 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. Effective leveraging of activity, resources and knowledgebase of a broad and deep community of interest. Efficient exchange of situational awareness and intelligence information.

6. **What metric or measurement will be used to define success?**
   a. Number of organizations collaborating in the effort, number of information and alert exchanges, number of meetings, and activities.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☒ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. The public; state and local election officials and administrators.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. Because a number of federal, state, industry and even public organizations are directing resources to election security, the Election Committee recognized the potential for significant overlap. A key aspect of the collaboration effort is to minimize programing overlap, allowing organizations to focus attention and resources on specific, rather than general aspects of election security.

## 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?**
    - DHS, DOD, US Cyber Command
    - Center for Internet Security

- Election Infrastructure Information Sharing and Analysis Center
- MS-Election -ISAC
- Cybersecurity and Infrastructure Security Agency Election Security Initiative
- National Association of Secretaries of State
- National Association of State Election Directors
- U. S. Election Assistance Commission (EAC)
- Indiana Fusion Center
- Indiana Executive Council on Cybersecurity
- Association of the Clerks of the Circuit Courts of Indiana
- Indiana Statewide Voter Registration System Core Team
- Indiana Voting System Technical Oversight Program (VSTOP)
- Indiana Voter Registration Association
- EAC accredited Voting System Testing Labs (VSTLs)
- Association of Government IT Leaders (GMIS.org)

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

a. The Secretary of State, Indiana Election Division and Statewide Voter Registration System Core Team (SVRS Core Team).

**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?

☐ One-time deliverable

☒ Ongoing/sustained effort

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Establishing collaboration | Secretary of State | 100 | No Response | |
| Participation in meetings and exchanges | Secretary of State/Election Division/SVRS Core Team | 100 | No Response | |
| Technical monitoring | Secretary of State/Election Division/SVRS Core Team | 100 | No Response | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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 |
|---|---|---|---|---|---|---|
| No new resources required. | | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Framework for rapid sharing of threat information and rapid response.

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

a. As a result of collaborative effort, focus of resources, and focus of attention, cybersecurity risk should be reduced across the election sector.

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

a. Increased risk of zero-day attack, inefficient utilization of resources due to activity overlap, longer response to threat time.

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

a. Efficiency in utilization of resources, organizational time and effort efficiency, communication of threat and response lead times.

**21. 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. Through the efforts of the National Association of Secretaries of State, many, if not all state election officials are engaging in a collaborative approach to election security.

**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?**

☒No ☐ Yes

## Other Implementation Factors

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

a. Collaboration mitigates inefficiency resulting from duplicative and overlapping efforts. The Committee is not aware of factors that might have a negative impact on collaboration between organizations.

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

☒No ☐ Yes

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

a. Collaboration is expected to be an easily and efficiently sustainable activity.

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

a. See response to question #11 above.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes,

a. Any sector should benefit from collaborative effort.

## Communications

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

a. Not applicable because key stakeholders are involved in a collaborative effort.

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

☐No ☒ Yes

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

a. Understanding of the number of organizations, collaborative effort, and resources focused on the effort can help alleviate public concern about election security and serve to dissuade threat actors.

## *Evaluation Methodology*

**Objective 1:** The new Secretary of State will actively engage with allied organizations indicated in the state's strategic plan by December 31, 2021.

*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 Secretary of State will continue engage in election cybersecurity collaboration with allied organizations every year as appropriate.

*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: Integration of Cybersecurity Professionalism, Awareness, and Practice

# Deliverable: Integration of Cybersecurity Professionalism, Awareness, and Practice

## *General Information*

1. **What is the deliverable?**
    a. Integration of Cybersecurity Professionalism, Awareness, and Practice

    - The Secretary of State will promote integration of experienced, trained, and professionally certified cybersecurity resources into all phases of election administration.
    - State and local election officials and administrators will be encouraged to engage Certified Information Security Professionals, and provide ongoing cybersecurity awareness, training, and certification opportunities for staff.
    - The Secretary of State will assist VSTOP with the integration of election cybersecurity into the Election Administration Certificate Program (CEATS).

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?**

☐ 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. Integration of experienced, trained and professionally certified cybersecurity resources into all phases of election administration.

6. **What metric or measurement will be used to define success?**
    a. Number of counties (local election administration units) employing, accessing or otherwise utilizing professional cybersecurity resources.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☒ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. The public, and state and local 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, Indiana Election Division and Statewide Voter Registration Core Team (SVRS Core Team).

13. **What are the expected challenges to completing this deliverable?**
    a. Possibly local government funding.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Encouragement | Secretary of State, Indiana Election Division, SVRS Core Team | ? | N/A | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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 |
|---|---|---|---|---|---|---|
| Local government funding. | Improved, more reliable security outcomes. | Unknown | Unknown | Local Government | State and Federal funding | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Improved, more reliable election cybersecurity outcomes

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

a. Qualified IT and cyber security professionals will have greater situational awareness, higher and faster threat response capability, improved day-to-day collaboration and maintenance of effort.

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

a. Lower situational awareness, slower threat response and capability, lower day-to-day collaboration, and maintenance of effort.

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

a. Number of counties (local election administration units) employing, accessing or otherwise utilizing professional cybersecurity resources.

**21. 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. Unknown. Possible survey subject.

**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?**

☐No ☒ Yes

a. Unknown. Possible survey subject.

## Other Implementation Factors

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

a. IT and cybersecurity workforce training and workforce limitations.

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

☒No ☐ Yes

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

a. Local government funding for maintenance of effort.

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

a. This deliverable is a topic of discussion within the election sector.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. Security outcomes in all sectors would likely be improved through institutionalizing employment of qualified IT and cybersecurity professionals.

## Communications

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

a. All election sector stakeholders should be kept abreast of effort and accomplishment in this area.

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

☐No ☒ Yes

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

a. Understanding of the utilization of IT and cybersecurity professionals in election administration can help alleviate public concern about election security and serve to dissuade threat actors.

## *Evaluation Methodology*

**Objective 1:** The Secretary of State will promote integration of experienced, trained, and professionally certified cybersecurity resources into all phases of election administration by November 2024.

*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:** More than 80 percent of state and local election officials and administrators will provide ongoing cybersecurity awareness, training, and/or certification opportunities by November 2024.

*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 Infrastructure Monitoring, Hardening, Testing, and Auditing

# Deliverable: Election Infrastructure Monitoring, Hardening, Testing, and Auditing

## *General Information*

1. **What is the deliverable?**
    a. Election Infrastructure Monitoring, Hardening, Testing and Auditing
        - The Secretary of State will promote election infrastructure cyber security monitoring and improvements in the following aspects:
            - Monitoring with the use of state-of-the-art contractors and protocols
            - Hardening via technical and process improvements
            - Voting system and electronic poll book testing and certification protocols, and implementation of paper audit trail voting systems
            - Post-election risk-limiting audit program development, funding, and implementation

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?**
    ☐ 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. Robust and uniform utilization of technical cyber security products and protocols across state and local election administration platforms and networks.

6. **What metric or measurement will be used to define success?**
    a. A number of counties and election systems, platforms, and networks integrating state-of-the-art cybersecurity tools and monitoring systems.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☐ 2022 ☐ 2023 ☒ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. The public, and state and local 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, Indiana Election Division, Statewide Voter Registration Core Team (SVRS Core Team).

13. **What are the expected challenges to completing this deliverable?**
    a. Local government funding.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Awareness | Secretary of State, Indiana Election Division, SVRS Core Team | 75 | 05/01/2024 | |
| Implementation | Secretary of State, Indiana Election Division, SVRS Core Team | 75 | 05/01/2024 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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 |
|---|---|---|---|---|---|---|
| The Secretary of State and Election Division are providing tools and services to counties with federal and state funding. | Additional resources are nor needed at this time. | No Response | No Response | No Response | No Response | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Higher level of IT and cybersecurity through uniform, proactive deployment of state-of-the-art security and monitoring tools and services.

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

a. Proactive investment in deterrence, early detection and fast response tools, and monitoring will likely be less costly and more supportive of public confidence than after-the-fact responses to security breaches.

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

a. Higher degree of sector network and infrastructure vulnerability, longer detection and response times, lower public confidence in election efficiency and outcomes.

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

a. Number of counties, election platforms, and networks utilizing the tools and monitoring services

**21. 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

**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?**

☐No ☒ Yes

## Other Implementation Factors

---

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

a. Local government units and IT administrator evaluation, approval, implementation, and collaboration.

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

☒No ☐ Yes

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

a. Sustained collaboration with local government and county election officials and administrators, sustained funding.

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

a. Active engagement on implementation of this deliverable across the election sector is ongoing.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. All sectors utilizing IT platforms and networks would likely benefit from utilization of state-of-the-art security tools and monitoring services.

## Communications

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

a. All election sector stakeholders should be kept abreast of effort and accomplishment in this area.

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

☐No ☒ Yes

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

a. Understanding of the utilization of state-of-the-art security tools and monitoring services in election administration can help alleviate public concern about election security and serve to dissuade threat actors.

## *Evaluation Methodology*

**Objective 1:** The Secretary of State will promote election infrastructure monitoring, hardening, testing, and auditing improvements every year until December 2024.

*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: Public Engagement and Confidence

# Deliverable: Public Engagement and Confidence

## *General Information*

1. **What is the deliverable?**
    a. Public Engagement and Confidence
        - The Secretary of State will maintain a high level of public engagement in the area of election security and public confidence including:
            - Surveying the public about election security and integrity concerns
            - Voter outreach, education, and engagement activities
            - Implementation of Internet enabled absentee voting and assistive technology for blind and print disabled voters

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?**
☒ 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. Continuously and routinely informing the public of the high level of federal, state, and local engagement in, and commitment to election security.

6. **What metric or measurement will be used to define success?**
    a. Surveys of public concerns and confidence.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☒ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. The public, and state and local 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, Indiana Election Division, Statewide Voter Registration Core Team (SVRS Core Team).

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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Surveys, communications activities | Secretary of State, Indiana Election Division, SVRS Core Team | 75 | No Response | No Response |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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 |
|---|---|---|---|---|---|---|
| No new resources required | | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Increased/sustained public confidence in election outcomes. High participation in elections.

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

a. Sustained awareness efforts can improve public engagement in cybersecurity awareness and effort.

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

a. Lower public confidence in election outcomes. Public stress and anxiety. Lower participation in elections.

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

a. Responses to public surveys.

**21. 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. 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?**

☐No ☒ Yes

a. Unknown

## Other Implementation Factors

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

a. Commitment of state and local election official and administrator time and communications resources.

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

☒No ☐ Yes

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

a. Ongoing commitment of state and local election official and administrator time and communications resources.

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

a. Stakeholders within the election sector are engaged in this initiative.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. All sectors would likely benefit from ongoing public communications and outreach activities.

## Communications

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

a. All election sector stakeholders should be kept abreast of effort and accomplishment in this area.

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

☐No ☒ Yes

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

a. None

## *Evaluation Methodology*

**Objective 1:** The Secretary of State will maintain a high level of public engagement in the area of election security and public confidence by November 2024.

*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: Continuity, Coordination, Maintenance of Effort and Oversight

# Deliverable: Continuity, Coordination, Maintenance of Effort and Oversight

## *General Information*

1. **What is the deliverable?**
    a. Continuity, Coordination, Maintenance of Effort, and Oversight
        - To assure the highest level of ongoing election cybersecurity vigilance and effort, the Secretary of State may integrate the IECC Election Committee's day-to-day, and election-to-election responsibilities with the professionally managed Indiana Statewide Voter Registration System Core Team.

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.**
☒ 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 Statewide Voter Registration System Core Team (SVRS Core Team) will oversee and coordinate IECC Election Committee activity and deliverables.

6. **What metric or measurement will be used to define success?**
    a. Ongoing effective and efficient coordination and execution of Election Committee business and deliverables.

7. **What year will the deliverable be completed?**
    ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. The public, and state and local 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, Indiana Election Division and SVRS Core Team.

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?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Transfer Election Committee administration to SVRS Core Team | Secretary of State, Election Division and SVRS Core Team | 50 | 12/31/2021 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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. Increased efficiency and responsiveness. The SVRS Core Team is continually active, has professional administrative and technical support resources, is bi-partisan, and typically meets on a bi-weekly basis.

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

a. Increased efficiency and responsiveness. See the SVRS Core Team response in #17.

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

a. None

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

a. Acceptance by the SVRS Core Team of responsibilities associated with administration of IECC Election Committee administration.

**21. 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

**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?**

☒No ☐ 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**?

☒No ☐ Yes

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

a. Possibly the SVRS Core Team will require additional administrative and technical support resources – likely provided by the Secretary of State and Indiana Election Division, on an as-needed basis.

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

a. Secretary of State, Indiana Election Division, SVRS Core Team.

**27. Can this deliverable be used by other sectors?**

☒No ☐ Yes,

## Communications

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

a. IECC leadership, state and local 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)?**

☐No ☒ Yes

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

a. None

## *Evaluation Methodology*

**Objective 1:** Indiana Statewide Voter Registration System Core Team will begin formally coordinating and overseeing the deliverables of the IECC Elections Committee Strategic Plan by Dec. 31, 2021.

*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 Statewide Voter Registration System Core Team will assist with all the deliverables and objective in the IECC Elections Committee Strategic Plan and report the progress to the IECC by Dec. 31 of each year.

*Type:* ☐ Output ☒ Outcome

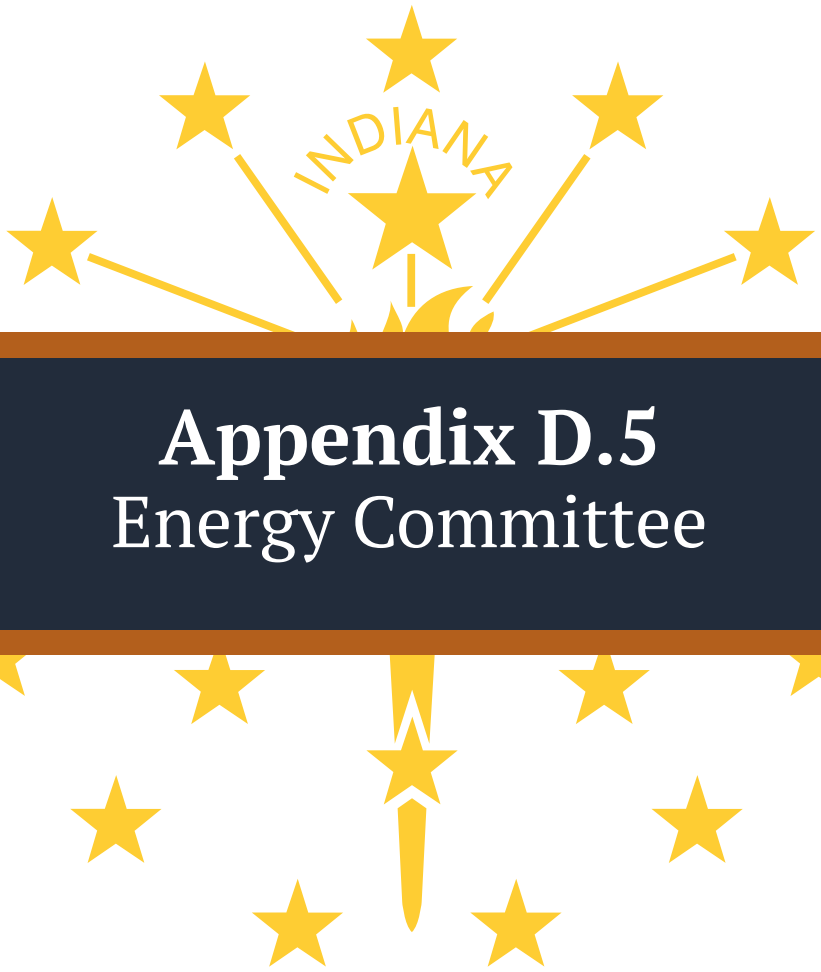
*Evaluative Method:*

☒ 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

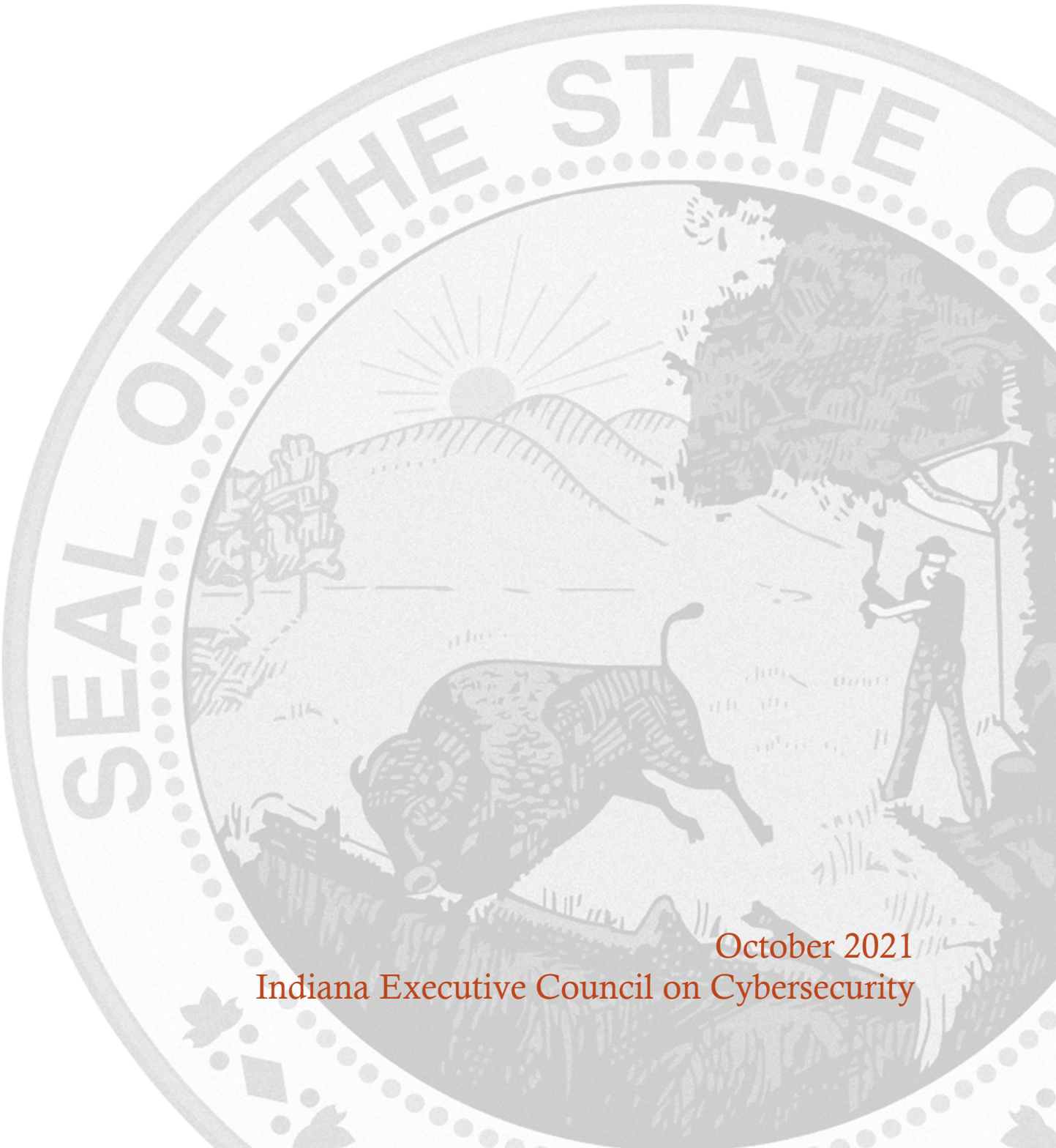
There was no supporting documentation at this time.




# Appendix D.5
## Energy Committee

# ENERGY COMMITTEE STRATEGIC PLAN

Chair: Danielle McGrath
Co-Chair: Robert I. Richhart



October 2021
Indiana Executive Council on Cybersecurity

# Energy Committee Plan

# Table of Contents

# Committee Members

# Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Aikman | J. Kurt | MISO Energy | Senior Security Advisor | Full Time |
| Berry | Scott | Indiana Municipal Power Agency | Compliance Manager | Full Time |
| Bowen | Brandon | Indiana Utility Regulatory Commission | Senior Utility Analyst | As Needed |
| Bowers | Scott | Hoosier Energy REC | Sr. VP Government and Community Relations | Full Time |
| Brown | Allen | Midwest Natural Gas | IT Director | Full Time |
| Cassady | John | Wabash Valley Power | Executive Vice President, Public Policy & Advocacy | Full Time |
| Chrislip | Chris | EICORP | Senior Cybersecurity Architect | As Needed |
| Dessuit | Frank | NIPSCO | Ops Technology and Security Manager | Full Time |
| Ellis | Greg | Indiana Chamber of Commerce | Vice President, Energy and Environmental Policy | Full Time |
| Garmon | Joe | Wabash Valley Power | Director of IT Policy and Cyber Security | Full Time |
| Willis | Corey | Indiana Electric Cooperatives (IEC) | VP, Information Services | Full Time |
| Hadley | Ryan | Indiana Utility Regulatory Commission | Executive Director of External Affairs | As Needed |

| | | | | |
|---|---|---|---|---|
| Holmes | Evan | CenterPoint | Manager, Control Systems | Full Time |
| Krevda | Stefanie | Indiana Utility Regulatory Commission | Commissioner | As Needed |
| McGrath | Danielle | Indiana Energy Association | President | Chair |
| Richhart | Robert | Hoosier Energy REC | Chief Technology Officer | Co-Chair |
| Souza | Tony | Duke Energy | Director, Cybersecurity Architecture, IT/OT & TVM | Full Time |
| Swick | Steve | American Electric Power (AEP)/Indiana Michigan Power (I&M) | Chief Security and Privacy Officer | As Needed |
| Taylor | Curtis | Wabash Valley Power | Executive Vice President, Technology Services | Full Time |
| Wright | Carolyn | Indiana Municipal Power Agency | Vice President, Government Relations | Full Time |
| Miller | Scott | Citizens Energy Group | Manager of Security and Compliance | Full Time |
| Bailey | Gerry | Corvano LLC | President | As Needed |
| Day | David | MISO Energy | Consulting Information Security Analyst | Full Time |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

# 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)
  - Assessed state-level guidelines
  - Reviewed National Association of Regulatory Utility Commissioners (NARUC) Cybersecurity Manual
  - Formulated needs for training by educational institutions to provide cybersecurity professionals
  - Determined level of interaction and need for interaction with other subsectors
  - Researched 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.
  - NARUC has resources for public utility commissions to gather and evaluate information from utilities about their cybersecurity risk management and preparedness.
  - On the national level, the Electric Subsector Coordinating Council and Oil & Natural Gas Subsector Coordinating Council are both quite active.
  - According to the National Conference for State Legislatures, the most commonly introduced bills seek to establish a state-level committee dedicated to studying cybersecurity and providing policymakers with recommendations.
  - Electric ISAC and Downstream Natural Gas ISAC are active.
  - Significant need for education and training exists.
  - Other subsectors, including for example Telecommunications and Financial, need to interact.

- **Committee Deliverable**
  - Critical Infrastructure Information (CII)
  - Training
  - Indiana Utility Regulatory Commission (IURC) Cybersecurity Forum
  - Resource Guide
  - Deliverable Workplace IT

- **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 broader economy and well-being of Hoosiers. This industry is also heavily regulated, including cybersecurity. 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 a training exercise is Grid-Ex. Grid-Ex is a biannual, nation-wide exercise which provides utilities a chance to "experience" a cyberattack. GridEx V in 2019 included more than 500 electric utilities, government and law enforcement agencies, and other organizations. GridEx VI is scheduled for November 16–17, 2021.
    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 includes downstream natural gas distribution companies 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. Communication between sectors (e.g., threats that are detected by another sector that others should be aware of)
    c. Potential disruptions of the telecommunications networks

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. There is continued 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). The TSA announced in July 2021 the issuance of a second Security Directive. This directive requires owners and operators of designated critical pipelines that transport hazardous liquids and natural gas to implement specific mitigation measures to protect against ransomware attacks and other known threats to information and operational technology systems. Critical Pipelines are also required to develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review. This is the second Security Directive that TSA has issued to the pipeline sector in 2021.

    The May 2021 Security Directive requires critical pipeline owners and operators to:
        1. report confirmed and potential cybersecurity incidents to CISA;
        2. designate a Cybersecurity Coordinator to be available 24 hours a day, seven days a week
        3. review current practices; and,
        4. identify any gaps and related remediation measures to address cyber-related risks and report the results to TSA and CISA within 30 days.

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. This training exercise is known as GridEx.

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 required to meet the same regulations or guidelines, training in the energy industry is similar across the country. , Energy utilities engage in national  and localized exercises.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Year One
        i. Energy providers of all sizes have access to cybersecurity resources for the purpose of bolstering their own internal cybersecurity plans.
        ii. Energy providers have identified unique workforce challenges for the industry associated the pandemic and identified best practices.
    b. Year Three
        i. Utilities have, if needed, modified and/or strengthened their cybersecurity plans.
        ii. Energy providers continue to understand, assess and implement protocols for dealing with the integration and security associated with new technology.
        iii. The energy providers and the IURC have established communication channels for sharing cybersecurity information.
        iv. Contact lists are maintained and updated as needed.
    c. Year Five
        1. Ongoing evolution of the way we work together in Indiana has revised and changed as we respond to the ever-changing risk environment.
        2. Utilities have an ever-increasing number of graduates from Indiana educational institutions who 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. Indiana's educational institutions should be more intentional about training students for cybersecurity roles. Educational institutions need to increase awareness of the importance of these roles and alert students to the types of jobs available in the field.

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
        - More than 12,000 direct employees.
    b. Cybersecurity-related workforce
        - More than 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. Best practices will be better assessed and implemented once more information on the current cybersecurity in other sectors is known. , 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 facilitate implementation.

# Deliverable: Critical Infrastructure Information (CII)

# Deliverable: Critical Infrastructure Information (CII)

## *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?**
☒ Completed ☐ In-progress 25% ☐ In-progress 50%. ☐ In-progress 75%. ☐ Not Started

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. In 2018, the Energy Committee determined that additional laws or policies were not needed in Indiana. We are conducting a new review to determine whether policy action is warranted now and will be examining different resources and engaging the broader energy industry.

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?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Customers, energy companies, law enforcement, disaster response personnel, media, and many others would benefit.

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 implemented mandatory regulations and/or guidelines which impact companies across the nation and 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 almost all Hoosiers use of electricity and natural gas, 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 Danielle McGrath at the Indiana Energy Association. It is her 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. None.

## *Implementation Plan*

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

☒ One-time deliverable

☐ Ongoing/sustained effort

### 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% | 9/30/21 | |
| Engage statewide energy industry stakeholders to determine whether state-level policy changes are warranted. | Indiana Energy Association<br>Indiana Municipal Power Agency<br>Indiana Electric Cooperatives<br>Indiana Chamber<br>Indiana Utility Regulatory Commission | 75% | 12/2021 | |

### Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| None | 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. 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 are 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 arise 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.

**21. 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

**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?**

☒No ☐ Yes

## 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 is already a part of the energy industry cost structure.

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

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. 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)?**

☐No ☒ Yes

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

a. We do not see this item as key for either public relations or marketing consideration.

## *Evaluation Methodology*

**Objective 1:** IECC Energy Committee will provide a review of the July 2018 definitions by October 2021.

*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 review potential state policy changes to protect critical infrastructure information while maintaining public access and freedom of information by December 2021.

*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. Training
        i. Objective 1: Develop a survey to determine whether there are new training needs specific to the energy industry following the pandemic.
        ii. Objective 2: Identify and recommend opportunities at the state, vocational, or higher education level.

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?**
    ☐ 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 the energy industry needs in training and education to support and enhance energy company cybersecurity, including identifying skill gaps and recommending opportunities to address them.

6. **What metric or measurement will be used to define success?**
    a. Identified training resources for identified training needs.

7. **What year will the deliverable be completed?**
    ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. All energy sector entities of various sizes.

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. Workforce Development Committee. Feedback from energy sector survey participants.

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. DHS, CISA, educational institutions and etc.

12. **Who should be the main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Danielle McGrath at the Indiana Energy Association. It is her 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?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Coordinate with Workforce Development Committee. | Energy Committee | 10% | 08/2021 | |
| Develop survey content. | Energy Committee | 0% | 08/2021 | |
| Distribute survey. | Energy Committee | 0% | 09/2021 | |
| Analyze results | Energy Committee | 0% | 10/2021 | |
| Research training opportunities to meet gaps | Energy Committee | 0% | 11/2021 | |
| Develop recommendations. | Energy Committee | 0% | 12/2021 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| Minimal | Minimal | Project Management | 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. Address training gaps to promote reliability and resiliency.

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.

19. **What is the risk or cost of not completing this deliverable?**
    a. Insufficiently trained employees.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Success is having Hoosiers who possess the skills the energy industry needs.

21. **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

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?**
    ☐No ☒ 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?**
    ☒No ☐ Yes

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. Annual review

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. In responses to the questions asked in Phase 1, we have asked for support from the Workforce Development Committee.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. 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)?**

☐No ☒ Yes

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

a. It would be an opportunity to highlight Indiana's educational system's ability to train individuals in an evolving technical workplace.

## *Evaluation Methodology*

**Objective 1:** Develop a survey to determine whether there are new training needs specific to the energy industry following the pandemic by October 2021.

*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:** Identify and recommend opportunities at the state, vocational, or higher education level December 2021.

*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: IURC Cybersecurity Forum

# Deliverable: IURC Cybersecurity Forum

## *General Information*

1. **What is the deliverable?**
    a. Host a forum for small natural gas utilities to share information and best practices on cybersecurity.

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?**
    ☐ Establish an effective governing structure and strategic direction.
    ☒ Formalize strategic cybersecurity partnerships across 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 purpose of the goal is to assess small gas operators' (less than 35,000 customers) cybersecurity preparedness and provide tools, resources, and information to guide them towards a greater understanding of their cybersecurity needs.

6. **What metric or measurement will be used to define success?**
    a. Completion rate of survey(s) and attendance at the in-person forum.

7. **What year will the deliverable be completed?**
    ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. IURC-regulated public gas utilities that serve generally less than 35,000 customers.

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. 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 Department of Homeland Security (IDHS), U.S. Department of Homeland Security (U.S. DHS), the Indiana Energy Association (IEA), the American Gas Association (AGA), the U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA), and the invited utilities, including:
        - Boonville Natural Gas Corp.
        - Community Natural Gas Go., Inc.
        - Fountaintown Gas Co., Inc.
        - Indiana Natural Gas Corp.
        - Midwest Natural Gas Corp.
        - Ohio Valley Gas Corp.
        - South Eastern Indiana Natural Gas Co., Inc.
        - Sycamore Gas Co.
        - Switzerland County Natural Gas Co.

12. **Who should be main lead of this deliverable?**
    a. Stefanie Krevda, IURC/Ryan Hadley, IURC

13. **What are the expected challenges to completing this deliverable?**
    a. Securing expert speakers for the event; setting an appropriate date for the forum that all parties can attend.

## *Implementation Plan*

**14. Is this a one-time deliverable or one that will require sustainability? Within the Commission we plan to regularly engage with our regulated utilities regarding cybersecurity matters; however, for the IECC sub-committee it will not.**

☒ One-time deliverable

☐ Ongoing/sustained effort

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Develop cybersecurity survey and send to small gas operators | Stefanie Krevda/Ryan Hadley | 100% | 6/4/2021 | Confidential survey sent and responses received by most gas operators on June 4, 2021. |
| Evaluate responses and develop list of topics for forum | Stefanie Krevda/Ryan Hadley | 25% | 8/1/2021 | |
| Set date and time for cyber forum | Stefanie Krevda/Ryan Hadley | 0% | 9/1/2021 | |
| Secure speakers for cyber forum | Stefanie Krevda/Ryan Hadley | 0% | 10/31/2021 | |
| Host cyber forum | IURC | 0% | Qtr. 1 2022 | |

### Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| None | None | | This type of work is already captured in the IURC and energy provider budgets. | | |

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

a. No Response

| 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 greatest benefit of the deliverable is two-fold: (1) education for regulators and small gas operators; and (2) provide resources for small gas operators to develop more mature cybersecurity protocols, as they determine applicable for their organizations.

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

a. The deliverable will reduce cybersecurity risk by educating small gas operators on the importance of evaluating and incorporating appropriate cybersecurity measures to mitigate risks and impacts to their systems. The estimated costs associated with risk reduction can range depending on the implemented steps, but likely in the thousands of dollars.

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

a. Cybersecurity risks can impose a great deal of costs if left vulnerable to attack. Small gas operators could lose their IT systems to ransomware, resulting in costs ranging in the thousands of dollars. However, if a cyberattack cripples their operational infrastructure, that could cost millions to replace, depending on the extent of the damages.

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

a. The baseline for evaluation is the survey results received from the small gas operators. The metric for success would be attendance at the in-person forum to hear from cybersecurity experts and increased cyber hygiene. Future cyber surveys will reveal an improvement their preparedness.

**21. Are there comparable jurisdictions (e.g., other states) that have similar projects using the same metrics?**

☒No ☐ Yes

**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?**

☒No ☐ Yes

## Other Implementation Factors

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

a. Generally speaking, any staff turnover at the IURC that impacts its ad-hoc cybersecurity working group may impact the requisite resources required to achieve the deliverable.

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

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. Water

## Communications

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

a. The Energy Committee of the IECC.

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

☐No ☒ Yes

*Note: The cybersecurity surveys and results should not be included as they are confidential and exempt from disclosure, but a summary and posting of the agenda of the Executive Session can be made available.*

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

a. We do not necessarily see this item as a key for either public relations or marketing consideration.

## *Evaluation Methodology*

**Objective 1:** Indiana Utility Regulatory Commission (IURC) will host a cybersecurity forum for small natural gas utilities to share industry information and best practices by December 2021.

*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: Resource Guide

# Deliverable: Resource Guide

## *General Information*

1. **What is the deliverable?**
    a. The deliverable is to develop a resource guide for all Indiana energy companies that helps identify emerging technology and supply chain issues and provides guidance and information to establish uniform and effective methods for cybersecurity protection across the entire energy sector.

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?**
☐ 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 development and sharing of a resource guide that informs all Energy Sector entities of uniform and effective policies, methods, and processes to protect their assets from malicious cybersecurity intrusions and potential system compromise.

6. **What metric or measurement will be used to define success?**
    a. A published resource guide for use by all energy sector entities.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. All energy sector entities

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. TBD

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. Key resources may include DHS CISA, EISAC, Indiana National Guard and possibly others.

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Danielle McGrath at the Indiana Energy Association. It is her 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. The everchanging threat landscape and acquiring resources. Developing comprehensive list of current resources for inclusion in resource guide.

# *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Gather information available across the sector and from other resources for development of the resource guide | Energy Committee | 25% | 3/1/2022 | |
| Develop Resource Guide | Energy Committee | 0% | Qtr. 3 2022 | |
| Disseminate Resource Guide | Energy Committee | 0% | Qtr. 4 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| None | | | | | |

**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. Sharing of knowledge, best practices, and resources regarding cybersecurity protection

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

a. Yes, the availability of this resource will help to reduce the potential cybersecurity risk by sharing information to help all energy sector entities to improve their cybersecurity protection processes in a uniform and effective manner.

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

a. Lack of awareness around industry best practices and resources

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

a. Improved awareness for all energy sector entities of best practices and processes to adequately protect against malicious cybersecurity incidents.

**21. 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

**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?**

☒No ☐ 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?**

☒No ☐ Yes

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

a. Annual review and refresh

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

a. No Response

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. Any critical sector

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

a. All energy utilities across state

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

☐No ☒ Yes

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

a. None

## *Evaluation Methodology*

**Objective 1:** The IECC Energy Committee will define emerging technology and supply chain issues related to the grid Qtr. 3 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

**Objective 2:** The IECC Energy Committee will determine whether best practices and information are widely available Qtr. 3 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

**Objective 3:** The IECC Energy Committee will develop an industry specific resource guide Qtr. 4 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: Workplace IT

# Deliverable: Workplace IT

## *General Information*

1. **What is the deliverable?**
    a. To develop a survey to capture cybersecurity challenges that the energy sector has faced as a result of workforces moving to work-from-home models. Identify best practices within the survey respondents and/or industry standards and share those results with the energy sector.

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?**
    ☐ 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. Increased awareness within the energy sector of the challenges introduced by a remote workforce and awareness of best practices to address those challenges.

6. **What metric or measurement will be used to define success?**
    a. The dissemination of survey results and industry best practices.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Energy sector and partners in similar industries

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 Energy Association, Indiana Electric Cooperatives, Indiana Municipal Power Agency

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Danielle McGrath at the Indiana Energy Association. It is her 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. Asking the correct questions in the survey and targeting the correct audience

## *Implementation Plan*

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

☒ One-time deliverable

☐ Ongoing/sustained effort

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Develop survey content | Energy Committee | 0% | 08/2021 | |
| Distribute survey | Energy Committee | 0% | 09/2021 | |
| Analyze results | Energy Committee | 0% | 10/2021 | |
| Identify trends/best practices in survey responses | Energy Committee | 0% | 11/2021 | |
| Identify industry best practices (NIST, CERT) to reference for best practices | Energy Committee | | 12/2021 | |
| Develop and distribute recommendations. | Energy Committee | 0% | 2/2022 | |

### Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| 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.)**

**a.** No Response

| 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

**17. What is the greatest benefit of this deliverable?**

**a.** Providing energy sector members with best practices and industry resources to manage a remote workforce.

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

**a.** By establishing better processes and controls to manage the risk of a remote workforce. Costs of implementing such measures will be unique to each organization.

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

**a.** Increased cyber risks to the energy sector due to poorly controlled and managed remote workforce.

**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 by providing energy sector member with the tools and resources to better mitigate cyber risks.

**21. 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

**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?**

☒No ☐ 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?**

☒No ☐ Yes

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

a. Not ongoing

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

**a.** Workforce Development

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

**a.** Water/Wastewater Sector and other sectors with industrial control systems

## Communications

---

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

**a.** Energy Sector and Workforce Development

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

☒No ☐ Yes

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

**a.** Coordinating with industry groups to distribute the survey

## *Evaluation Methodology*

**Objective 1:** The IECC Energy Committee will develop a survey to identify challenges in the workplace for the energy sector in Qtr. 4 2021.

*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 IECC Energy Committee will identify issues stemming from the work-from-home environment in Qtr. 4 2021.

*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:** The IECC Energy Committee will share best practices and coordinate with other sectors as needed in Qtr. 1 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

# Supporting Documentation

# Supporting Documentation

This section contains all 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 – July 2021
- Electricity Subsector Coordinating Council (ESCC) - Cyber Mutual Assistance Program Brochure - January 2021
- Federal Energy Regulatory Commission (FERC) Critical Energy/Electric Infrastructure Information (CEII) Regulations - 2020 - 2020

# American Public Power Association (APPA) – *Cybersecurity and the Electric Sector*

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

**ISSUE BRIEF** June 2021

# Grid Security

## Summary

A reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans. Public power utilities, together with the entire electric utility industry, take very seriously their responsibility to maintain a secure and reliable electric grid. It is the only critical infrastructure sector that has mandatory and enforceable federal regulatory standards in place for cyber and physical security (collectively known as grid security). Cyber-attacks, relatively new compared to long-known physical threats, have rapidly evolved and could have operational consequences. The American Public Power Association (APPA) believes that the industry and its federal government partners have made great strides in addressing cybersecurity threats, vulnerabilities, and potential emergencies. Given the persistence and sophistication of threats, APPA knows that utilities cannot prevent all attacks at all times. For both cyber and physical threats, electric utilities employ risk management programs to prioritize facilities and equipment, develop contingency plans, and employ defense-in-depth techniques to keep the lights on.

## Key Pillars of Grid Security

### Mandatory and Enforceable Standards

The electric utility sector is the only critical infrastructure sector (besides the nuclear power sector, a part of the overall sector) that has a 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 (EPAct05) (section 215 of the Federal Power Act (FPA)). Under section 215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities, and government representatives, regularly drafts reliability, physical security, and cybersecurity standards that apply across the North American grid, including Canada.[1] Participation by industry experts and compliance personnel in the NERC critical infrastructure protection (CIP) 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, under FERC's oversight, NERC and its regional entities conduct 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.

CIP standards establish an important baseline of security—but they are a floor, not a ceiling—and grid security is and should be much more than a compliance exercise.

### Information Sharing

Industry 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, APPA strongly supported passage of the Cybersecurity Act of 2015, which was incorporated as Division N of

1 NERC standards cover the Bulk Electric System (BES).

P.L. 114-133, the Consolidated Appropriations Act, 2016. The act provides policies and procedures for sharing cybersecurity threat information between the federal government and private entities (which includes electric utilities), as well as sharing between private entities while providing limited liability protection for these activities if conducted in accordance with the act.

In addition to the Cybersecurity Act of 2015, APPA also strongly supported section 61003 of P.L. 114-94 (the Fixing America's Surface Transportation Act or "FAST Act"), which gave the Secretary of Energy broader authority to address grid security emergencies under the FPA. It also 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. Under the FAST Act, FERC-designated CEII is exempted from disclosure for a period of up to five years with a process to lift the designation or challenge it in court. In addition, it established sanctions for the unauthorized disclosure of shared information. It is critical to operational security that the industry is confident that sensitive information about critical infrastructure that might provoke new threats or endanger the integrity of the electric power grid not be publicized. CEII information in the public sphere creates a grave vulnerability to the electric power grid, by significantly reducing the surveillance effort required by dedicated domestic and foreign adversaries. APPA has supported legislation and actions by DOE and FERC that would further clarify and enhance the ability of the federal government and other stakeholders to maintain the confidentiality of CEII to minimize the risk that such information could be used by malicious actors to target grid infrastructure.

APPA strongly encourages its members to share physical security and cybersecurity related threats that they face to information sharing entities, such as the Electricity Information Sharing and Analysis Center (E-ISAC), as well as the Multi-State Information Sharing and Analysis Center. These information sharing organizations are critical to ensure that the broader public power community and the entire electric power industry have awareness of the tactics, techniques, and procedures used by the adversaries targeting the electric grid.

### Public-Private Partnerships

The electric power industry works closely with the federal government, including NERC, FERC, DOE, and the Department of Homeland Security (DHS), on matters of critical infrastructure protection. One important venue for this collaboration is the Electric Subsector Coordinating Council (ESCC). The ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. APPA and public power utilities play a leadership role on the ESCC, which includes utility CEOs and trade association leaders representing all segments of the industry. Their counterparts include senior administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

APPA works directly with DOE on a number of fronts. Most recently, in September 2020, DOE's Office of Cybersecurity, Energy Security and Emergency Response (CESER) awarded APPA a grant of $6 million over a three-year period to develop and deploy cyber and cyber-physical solutions for public power utilities. The program's goal is to provide utilities with emerging innovations at the hardware, firmware, and/or software levels to protect key operation technology (OT) components that enable the safe control of the physical systems that deliver electric power. This effort builds on the accomplishments of another three-year grant CESER awarded to APPA in 2016, with which APPA assessed and helped to strengthen the cybersecurity posture of small- and medium-sized public power utilities. This grant enabled the development of a cybersecurity scorecard for public power utilities to assess their cyber readiness, the production of a cybersecurity roadmap, an incident response playbook, and other guidance documents to help utilities develop a culture of cybersecurity within their organization.

Legislation based on the success of the 2016 grant program has been introduced over the past three Congresses. Most recently Representatives Jerry McNerney (D-CA) and Bob Latta (R-OH) introduced H.R. 2931,the Enhancing Grid Security through Public-Private Partnerships Act, to permanently fund

public-private partnerships to promote and advance the physical and cybersecurity of electric utilities. The House Energy & Commerce Committee approved H.R. 2931 unanimously in June. APPA strongly supports the bill. There is not currently a standalone Senate companion, but a similar provision is included in a draft infrastructure bill by Senate Energy & Natural Resources Committee Chairman Joe Manchin (D-WV).

### "Defense-in-Depth" and Sector-Wide Preparation Exercises

The goal of every utility and the entire industry is to manage risk prudently. Still, there are tens of thousands of diverse facilities throughout the U.S. and Canada that cannot be protected 100 percent of the time from all threats, requiring utilities to prioritize facilities that, if damaged, would have the most severe impacts on their ability to keep the lights on. As such, the electric power industry employs threat mitigation known as "defense-in-depth" that focuses on preparation, prevention, response, and recovery to "all hazard" threats to electric grid operations.

Electric utilities plan and regularly exercise for a variety of emergency situations that could impact their ability to provide electricity. One such exercise, GridEx V, took place in November 2019 and involved over 500 organizations and 7,000 participants from industry, government agencies, and partners in Canada and Mexico. APPA was significantly involved in the planning for GridEx V to further allow distribution utilities to get value from the distributed play portion of the exercise. One hundred public power organizations participated in the GridEx V distributed play, up from 53 that did so at GridEx IV in 2017. Managed by NERC and the E-ISAC, GridExV also included an executive tabletop exercise where 108 electric sector executives and senior U.S. government officials worked through incident response protocols to address widespread outages. GridEx events are conducted every two years; GridEx VI is scheduled for November 2021.

The three primary segments of the electric utility industry—public power, investor-owned, and rural electric cooperatives—have long had in place mutual aid response networks to share employees and resources to restore power after natural disasters and other emergencies. The ESCC used the concept of traditional mutual assistance networks to develop the Cyber Mutual Assistance program that can help electric and natural gas companies, public power utilities, and/or rural electric cooperatives restore critical computer systems following significant cyber incidents. The program now includes more than 170 entities across all segments of the industry, serving more than 80 percent of all U.S. electricity customers.

Finally, electric utilities regularly share transformers and other equipment through long existing bilateral and multilateral sharing arrangements and agreements. The industry is expanding equipment sharing programs—like the Spare Transformer Equipment Program (STEP), SpareConnect, and Grid Assurance—to improve grid resiliency.

## Administrative Action

### Supply Chain Security Executive Actions

On May 1, 2020, President Trump signed an Executive Order 13920 (EO or order), *Securing the United States Bulk Power System,* deeming "the unrestricted foreign supply of bulk-power system electric equipment" as an "unusual and extraordinary threat to national security." The order broadly prohibited any person subject to federal jurisdiction from acquiring, importing, transferring, or installing bulk-power system electric equipment designed, developed, manufactured, or supplied by foreign adversaries when those transactions pose an undue or unacceptable risk to the grid or national security. DOE was tasked with leading a broad inter-agency effort to further define and implement the order's requirements within 150 days. As part of the implementation of the EO, on December 17, 2020, DOE released a prohibition order aimed at reducing the risks that entities associated with China pose to the nation's BPS. The order, which took effect January 16, 2021, prohibited utilities that supply critical defense facilities from procuring from China specific BPS equipment that poses an undue risk to the BPS, the security or resilience

of critical infrastructure, the economy, national security, or safety and security of Americans. The order only applied to utilities that have been designated as defense critical electric infrastructure (DCEI); a small number of public power utilities have been notified that they have been designated as DCEI.

On his first day in office, President Joe Biden signed an Executive Order, *Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis,* that included a provision suspending EO 13920 for 90 days and directing DOE and the Office of Management and Budget to "jointly consider whether to recommend that a replacement order be issued." On April 20, DOE announced that it was revoking the December 17, 2020, prohibition order on securing critical defense facilities [EO 13920 itself was briefly reinstated following the 90-day suspension, but the emergency declaration of the EO expired on May 1]. In conjunction with the announcement that it was revoking the prohibition order, DOE announced a new request for information (RFI), "Ensuring the Continued Security of the United States Critical Electric Infrastructure," seeking input from stakeholders to inform future recommendations for supply chain security in U.S. energy systems. APPA submitted comments in response to the RFI on June 7, asking DOE to focus on four foundational principles as it considers further action on energy sector supply chain security: (1) new measures must be risked-based; (2) directives should be clear, prospective, and scalable; (3) directives must be cost-conscious; and (4) DOE should focus on vendor risks.

### NSC "100 Day Industrial Control Systems Cybersecurity Sprint"

On April 20, the Biden administration announced that it was launching a new initiative to enhance the cybersecurity of electric utilities' industrial control systems (ICS). This 100 day "sprint" is a coordinated effort between the National Security Council (NSC), DOE, and the ESCC to encourage and support utilities' visibility and situational awareness into their ICS and OT networks. APPA, as the primary public power point of contact for the initiative, is working with public power utilities to facilitate their participation in this voluntary pilot program. This effort has appropriately raised the issue of ICS security to a higher priority in the federal government. APPA views this sprint as the start of a long journey of collaboration between public power and the federal government, which includes the work being done through the CESER grant to APPA.

## APPA Position

The regulations and standards ("NERC-FERC") process set up in EPAct05 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, the industry recognizes that it 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.

## APPA Contact

Amy Thomas, Senior Government Relations Director, 202-467-2934 / athomas@publicpower.org

Jack Cashin, Director, Policy Analysis & Reliability Standards, 202-467-2979 / jcashin@publicpower.org

Nathan Mitchell, Senior Director, Operations Programs, 202-467-2925 / nmitchell@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) - Cyber Mutual Assistance Program Brochure*

# The ESCC's Cyber Mutual Assistance Program

The Electric Power and Natural Gas Industries Share Expertise to Counter Cyber Attacks

CMA
Cyber Mutual Assistance

## Cyber Defense: Building on the Industry's Culture of Mutual Aid

The North American energy grid is a complex interconnected network of generation, transmission, and distribution systems operated by thousands of organizations. Protecting the energy grid and ensuring a reliable and affordable supply of energy are the top priorities of the electric power and natural gas industries. Creating a "defense-in-depth" approach requires partnerships and coordination with the government and other critical infrastructure sectors. To coordinate security strategies with the federal government and other stakeholders, the electric power industry has created a CEO-led partnership called the Electricity Subsector Coordinating Council (ESCC).

For decades, the electric power and natural gas industries have operated voluntary mutual assistance programs that work collaboratively to restore service following storms, earthquakes, wildfires, and other natural disasters. These mutual assistance programs provide a formal, yet flexible, process for companies to request assistance from one another.

Building on the industries' culture of mutual assistance, and informed by lessons learned from major destructive cyber incidents overseas as well as by exercises held in North America, the ESCC directed the formation of the Cyber Mutual Assistance (CMA) Program. The Program is a natural extension of the electric power and natural gas industries' longstanding approach of sharing critical personnel and equipment when responding to emergencies. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power and natural gas industries are enhancing our nation's ability to defend and protect against threats and to meet customers' expectations.

## Delivering and Coordinating Cyber Mutual Assistance: How It Works

- The CMA Program is composed of industry cyber experts who are able to provide voluntary assistance to each other in advance of, or in the event of, a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency.
- Participation in the CMA Program is open to all entities that provide or materially support the provision of electricity or natural gas service.
- Participation in the CMA Program, as well as any decision to respond to requests for assistance made under the CMA Program, is voluntary.
- To participate in the CMA Program, entities must execute a mutual non-disclosure agreement so that all participants are assured that confidential information they may share will be protected.
- Participating entities also must designate an individual with appropriate cyber skills and experience, and the necessary authority, to represent the entity in the CMA Program (the CMA Coordinator).
- Cyber mutual assistance under the CMA Program is intended to be advisory and short-term. It may include services, personnel, and/or equipment.
- There is no cost to participate in the CMA Program other than the reimbursement of the costs and expenses of an entity providing emergency cyber assistance.

# Frequently Asked Questions About Cyber Mutual Assistance

**What is the Cyber Mutual Assistance Program?**

The Cyber Mutual Assistance (CMA) Program is an industry framework developed at the direction of the ESCC to provide emergency cyber assistance within the electric power and natural gas industries. The CMA Program is composed of industry cyber experts who can provide voluntary assistance to other participating entities in advance of, or in the event of, a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency. As the CMA Program develops, additional initiatives will be considered and implemented based on the needs and input of the entities participating in the CMA Program.

**How can I participate in the CMA Program?**

To participate in the CMA Program, each participating entity must (1) sign a mutual non-disclosure agreement, and (2) designate a CMA Coordinator.

**What does a CMA Coordinator do?**

A CMA Coordinator is a participating entity's primary point of contact for all matters related to the CMA Program. He or she is responsible for assessing relevant cyber resources, considering and responding to another participating entity's request for assistance, and making any requests for emergency assistance on behalf of the entity he or she represents.

**What are the qualifications for a CMA Coordinator?**

A CMA Coordinator must be an individual with sufficient authority to act on behalf of the participating entity he or she represents. In addition, a CMA Coordinator must possess or manage sufficient cybersecurity, operating technology, and information technology skills and experience to be able to request, or respond to a request for, a broad range of emergency cyber needs in the context of a potentially complex and evolving cyber emergency.

**How does the Program work?**

In the event of a cyber emergency, any participating entity may make a direct request for assistance through its CMA Coordinator to any other CMA Coordinator, or may make a broader request to multiple or all CMA Coordinators. Requests for assistance may be made in response to a particular cyber emergency or in advance of a threatened or anticipated cyber emergency.

**What kind of assistance is provided under the CMA Program?**

In responding to a request for assistance, a participating entity's response is voluntary, intended to be advisory in nature, and provided on a short-term basis. Assistance may include services, personnel, and/or equipment.

**Who is participating in the CMA Program?**

Currently more than 170 entities, representing electric and natural gas investor-owned companies, public power utilities, electric cooperatives, Regional Transmission Organizations and Independent System Operators, and Canadian energy companies, participate in the CMA Program. These entities cover approximately 80 percent of U.S. electricity customers, roughly 75 percent of U.S. domestic natural gas customers, and approximately 1.25 million electricity customers in Canada.

ESCC
Electricity Subsector Coordinating Council

**For more information about the CMA Program or to become a participant, please visit www.electricitysubsector.org/CMA or contact cma@electricitysubsector.org.**

# Federal Energy Regulatory Commission (FERC) Critical Energy/Electric Infrastructure Information (CEII) Regulations

# 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**, 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**, 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**, 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
  - Media Non-Disclosure Agreement
  - Federal Agency Acknowledgement and Agreement

**Order No. 662**, 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**, 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**, issued July 23, 2003
This Order requires companies to make information directly available to the public under certain circumstances.

**Order No. 630-A**, 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**, 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.

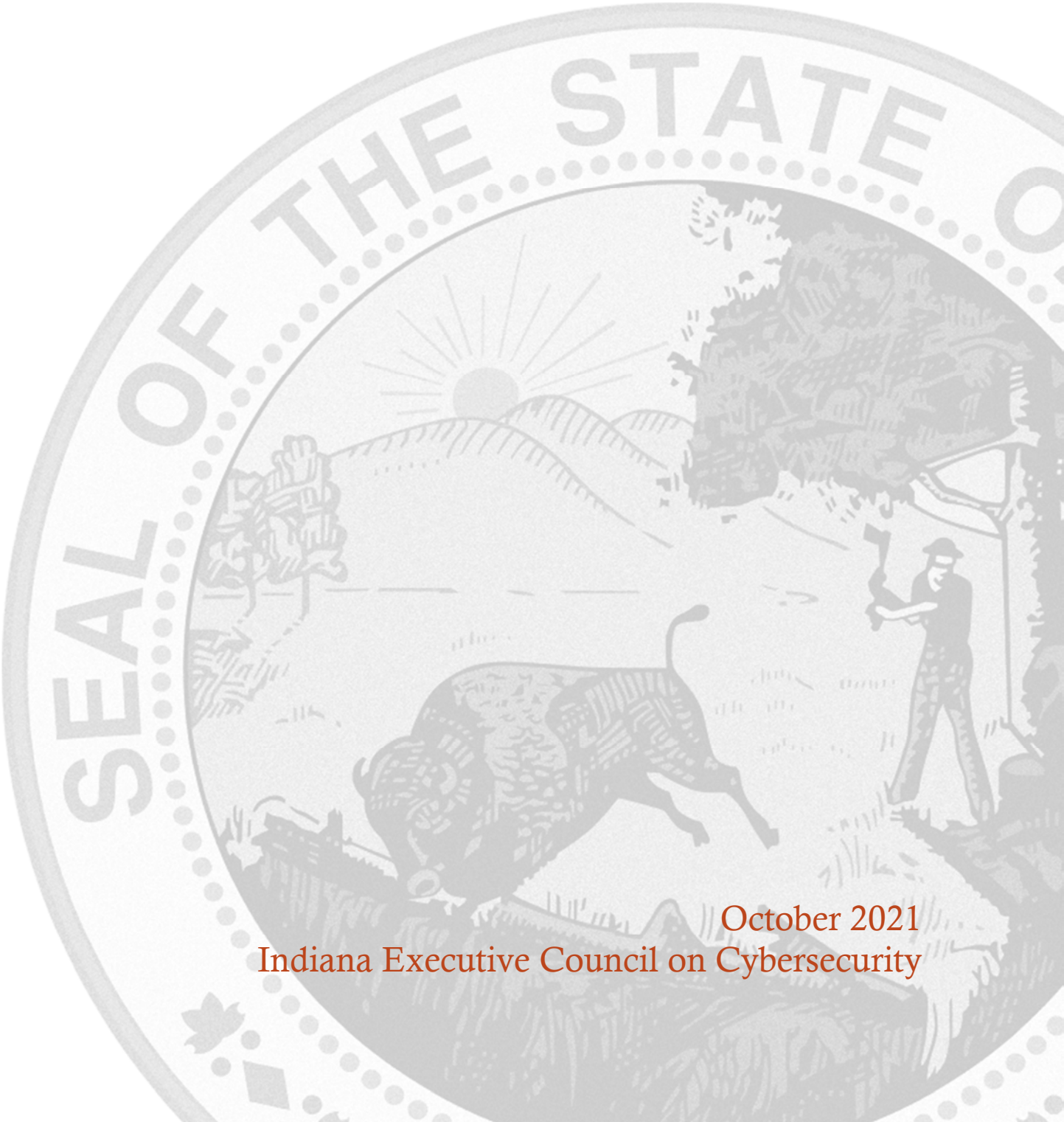
**PL02-1-000**, issued October 11, 2001
The September 11, 2001 terrorist attacks on America prompted the Commission to reconsider its treatment of certain documents that have previously been made available to the public through various means. The Commission removed from the public viewing certain documents, such as oversized maps, that detail the specifications of energy facilities licensed or certificated under Part I of the Federal Power Act, and Section 7(c) of the Natural Gas Act.

*This page was last updated on June 12, 2020*


# Appendix D.6
## Finance Committee

# FINANCE COMMITTEE STRATEGIC PLAN

Chair: Angie Ritchey
Co-Chair: Tom Fite




October 2021
Indiana Executive Council on Cybersecurity

# Finance Committee Plan

# Table of Contents

# Committee Members

## Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Cloud | Matthew | Ivy Tech Community College of Indiana-Lake County Campus | Director of Cybersecurity Grants, Asst. Prof. of Data Analytics, and Dept. Chair School of IT and Criminal Justice. | Full Time |
| Fite | Tom | Indiana Department of Financial Institutions | Director | Co-Chair |
| Goodlink | George | Lake City Bank | Director | Full Time |
| Hochstetler | Jay | Qumulus Solutions | Vice President, Security Operations | Full Time |
| Leetz | Tanya | People's Bank | Executive VP, Chief Information and Technology Officer | Full Time |
| Lodin | Steve | Sallie Mae Bank | Senior Director, Cybersecurity Operations | Full Time |
| Merkner | Karl | United Federal Credit Union | Security Engineer | Full Time |
| Ritchey | Angie | Lake City Bank | Senior Vice President, Chief Technology Officer | Co-Chair |
| Stouder | Kevin | Indiana Department of Financial Institutions | IT Examiner, IT Program Lead | Co-Chair Proxy |
| Wuellner | Mark | Indiana Bond Bank | Executive Director | As Needed |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan.*

For more information, visit www.in.gov/cybersecurity.

# Executive Summary

# Executive Summary

- **Research Conducted**
  - Determined the need for additional hands-on training and education of industry professionals based on information security best practices and procedures. Committee members also spoke to industry professionals, vendors, and researched common training courses targeted to the financial industry.

- **Research Findings**
  - There is still a need for increased and on-going training and education.

- **Committee Deliverables**
  - Board Leadership Education Plan
  - Disruption Plan
  - Top Security Tips Material 2.0

- **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. A number of those steps have included educating and training industry professionals through educational opportunities, professional organizations, as well as a number of informal discussions.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. There have been a number of significant cyber incidents that have affected the financial industry. Among the most notable have been Finastra and Kaseya ransomware attacks, SolarWinds supply-chain attack, Microsoft Exchange server attack, and Windows print spooler zero-day exploit. 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 towards following information security best practices to avoid risks.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. The greatest cybersecurity risk in the financial industry is the lack of education about cybersecurity. The risks are real, they do occur, and they have real consequences! We need to remain diligent in how we store, process, and transmit information. We must also hold people accountable for the confidentiality, integrity, and availability of data. One way to remain diligent is to continue to educate people. It is through cybersecurity education that the greatest awareness can be achieved.

4. **What federal, state, or local cyber regulations are 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 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 on page 9 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 Federal Financial Institutions Examination Council (FFIEC) published the Cybersecurity Assessment Tool (CAT) with the most recent version being May 2017. The CAT 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. Other similar tools include the Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile, which is now maintained, updated, and managed by the Cyber Risk Institute "CRI" and was last updated in November 2020. The CRI plans to release a number of new versions by the end of year 2021 that will also include a Cloud Controls version to its profile. The National Institute of Standards and Technology (NIST), under the Department of Commerce, has also created a Cybersecurity Framework (CSF). The framework is a voluntary guidance, based on existing standards, guidelines, and practices for organizations (not just in the financial sector) to better manage and reduce cybersecurity risk.

8. **What does success look like for your area in one year, three years, and five years?**
    a. It is difficult to define "success" within the cybersecurity space. With the advent of zero-day attacks, social engineering, or simple human failure, there are many reasons why cyber incidents continue to plague the financial sector. However, "success" may be achieved through greater education, collaboration, and communication.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. IT/Cybersecurity focused training is needed both in the corporate world and with individual citizens. Access to this training is key. Training is often targeted at IT/Cybersecurity specialists with minimal training available for non-IT staff. Furthermore, training can be expensive, leaving corporations in a quandary as to who should receive IT/Cybersecurity training and to what depth that training should cover. From a consumer standpoint, financial institutions also recognize that remote access to their customers' data poses a significant risk. To mitigate this risk, financial institutions need to remain diligent in educating customers on IT/Cybersecurity best practices. A customized information security curriculum targeted towards financial sector professionals and customers will increase awareness of IT/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 and affordability of these resources. Larger metropolitan areas have better access to staffing resources; however, demand for these resources is also greater in metropolitan areas.

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. Several different industry resources and best practices are available; however, none serves a one size fits all solution. Among the most notable non-industry specific IT/Cybersecurity and Risk resources include the National Institute of Standard and Technology (NIST); Cybersecurity and Infrastructure Security Agency (CISA); Center for Internet Security (CIS); and Information Systems Audit and Control Association (ISACA). Given the wide range of complexity and risks across the financial industry, it would be unlikely that any one set of best practices would fulfill the needs of all financial businesses.

# Deliverable: Board Leadership Education Plan

# Deliverable: Board Leadership Education Plan

## *General Information*

1. **What is the deliverable?**
    a. To provide formal cybersecurity training at a management or board membership level, outlining responsibilities associated with oversight within their organization. This formal training could and likely will be beneficial to all sectors of the IECC.

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?**
    ☐ 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. Executives/Leaders are better prepared to address the challenges presented to their organizations as a result of cyber threats.

6. **What metric or measurement will be used to define success?**
    a. Attendance and completion of the program.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. Any organization who participated in the training program.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None of which we are aware.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Possibly all other critical infrastructures committees 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. To be determined. There has been previous program development with Ivy Tech and that may be necessary or appropriate here as well.

12. **Who should be main lead of this deliverable?**
    a. IECC Member, George Goodlink

13. **What are the expected challenges to completing this deliverable?**
    a. Advertising this program to leadership across the state and gaining interest in participation.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Identify Curriculum | Committee | | 12/31/2021 | |
| Identify Instructor/Agency | Committee | | 3/31/2022 | |
| Advertise Program | IECC | | 6/30/22 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 3 | 6-10 | Role = ISO or CISSP | Volunteers | | CISSP certification requires CPE hours, which can include serving as an instructor for these types of courses, benefiting this deliverable as well as the CISSP. |

**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 |
|---|---|---|---|---|---|---|
| Materials | Training materials to be used as Guides | $2500 | $5000 | Grant funding | Could charge a fee to the attendees of their place of business. | Could potentially identify sponsors for the program |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Proper education of board members and leadership on the perils of cybersecurity and steps to take if impacted by an event.

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

a. Much of this depends on the extent of the event and costs associated with addressing the threat and recovery.

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

a. Same response as question 18.

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

a. Participation and completion rates.

**21. 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. Unsure as to where other programs exist.

**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?**

☐No ☒ Yes

a. Unsure as to any other programs that exist, but there are increasing threats associated with cybersecurity consistently reported by media. An assumption that boards are receiving this type of education, but only internally. This effort, however, would be sector wide.

## Other Implementation Factors

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

a. Lack of engagement, interest, or resource availability

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

☒No ☐ Yes

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

a. Consistent review of materials included in the program, updates to curriculum and a supply of CISSPs to present.

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

a. This is a new deliverable, so no outside contact or discussion has occurred.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. All sectors

## Communications

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

a. IECC and financial institutions in Indiana through associations and communication efforts

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

☐No ☒ Yes

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

a. An awareness campaign will be critical to the success of this program, including social media, news media, and local chambers.

## *Evaluation Methodology*

**Objective 1:** 1: IECC Finance Committee will develop a curriculum and identify an instructor(s) to be used for the Board and Executive Leadership Education Plan by June 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

**Objective 2**: The Board and Executive Leadership Education will be provided to a pilot group of finance institutions by December 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: Disruption Plan and Communication Evaluation

# Deliverable: Disruption Plan and Communication Evaluation

## *General Information*

1. **What is the deliverable?**
    a. Like all businesses, financial service providers are subjected to ongoing cyberattack attempts. Albeit rare, successful attacks present substantial risk of a disruption in consumer services, and awareness of this disruption could lead to panic for consumers. This distress could even lead to public safety concerns, such as a deposit run on an institution. Within this deliverable the committee will research the risk of financial services disruption. Any barriers to communication will be explored in effort to outline a communication plan institutions could deploy if/when they need support during and after a cyberattack.

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?**
    ☐ 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. This deliverable hopes to increase services and communication available should a cyberattack occur.

6. **What metric or measurement will be used to define success?**
    a. Success will be achieved with the creation of a disruption communication and support strategy primarily. However, it is anticipated that there will be many barriers to communication as well and mapping these barriers will likely become a secondary benefit of this deliverable.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☐ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. Financial service providers, financial services consumers, and government leadership.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Unknown. This is one of the questions that could be answered. A list of such resources may not presently exist.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. It is anticipated coordination may be necessary with other groups that involve security and emergency response.

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. Unknown. This question will be answered while completing this deliverable.

12. **Who should be main lead of this deliverable?**
    a. The Indiana Department of Financial Institutions in coordination with partners like the Indiana Bankers Association, the Indiana Credit Union League, and Indiana based federal regulators.

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

a. Confidentiality rules will be a substantial barrier for at least two reasons. Various laws and regulations protect financial service provider information and regulatory findings, and appropriately/importantly so. Revealing details about a cyber attack on a financial institution can make matters worse by revealing certain facts that assist cyber terrorists in further expanding the attack at the affected and/or additional institutions.

## *Implementation Plan*

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

☒ One-time deliverable

☐ Ongoing/sustained effort

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Begin mapping out the connections to the various partners in the finance sector at a federal, state, and local level | Indiana Department of Financial Institutions | - | 2022 | |
| Determine the proper channels and limitations of information sharing of key stakeholders | Indiana Department of Financial Institutions in coordination with partners like the Indiana Bankers Association, the Indiana Credit Union League, and Indiana based federal regulators | - | Qtr 3 2022 | |
| Develop a disruption plan for sharing information with key stakeholders including the State Emergency Operations Center | IECC Finance Committee with Cybersecurity Program Director | - | Qtr 4 2022 | |
| Circulate the disruption plan with all stakeholders | IECC Finance Committee with Cybersecurity Program Director | - | Qtr 3 2023 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| None | | | | | |

**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 at this time. | | | | | | |

## Benefits and Risks

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

a. The largest benefit is preparedness. Upon completion of this deliverable, there will be better understanding of access to public/private coordination during a cyber attack and more awareness of the impediments to communication following a successful attack.

**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 reduce the risk of a cyber incident. It will however assist with risk mitigation following any disruption that may occur stemming from a cyber attack.

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

a. Undetermined

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

a. Undetermined

**21. 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

**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?**

☒No ☐ Yes

## Other Implementation Factors

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

a. The ongoing pandemic continues to demand significant resources from the parties that will be involved with this deliverable. Many unknowns are still ahead for the financial services community, and any pandemic driven recessionary pressures would take human resources away from this deliverable.

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

☒No ☐ Yes

a. The response to question 24 is unknown at this time. No regulatory/policy change is anticipated, but this will become clearer during the work of this project.

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

a. Unknown.

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

a. No contact has been made as of yet, deliverable has not been started.

**27. Can this deliverable be used by other sectors?**

☒No ☐ Yes

## Communications

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

a. Regulatory leadership, financial services association leadership, and governmental leadership.

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

☒No ☐ Yes

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

a. None

## *Evaluation Methodology*

**Objective 1:** IECC Finance Committee will develop a Finance Sector Disruption Plan for the State of Indiana by Qtr. 3 of 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

**Objective 2**: The IECC Finance Committee will evaluate communication opportunities and identify associated barriers by Qtr. 4 of 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

# Deliverable: Top Security Tips Material 2.0

# Deliverable: Top Security Tips Material 2.0

## *General Information*

1. **What is the deliverable?**
    a. The IECC finance committee developed top security tips as a deliverable from the prior three-year strategic plan (see supporting documentation for Top Security Tips Material 1.0). The committee will now review these tips to be sure that they remain current and applicable. As with the first version of this material, the committee will 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?**
    ☐ Completed ☒In-progress 25% ☐ In-progress 50%. ☐ In-progress 75%. ☐ Not Started

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. Better end-user information security posture, education, awareness, reporting, and response.

6. **What metric or measurement will be used to define success?**
    a. Release of updated security tips that can be utilized by entities with limited IT resources.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. Local and State governmental entities throughout Indiana.
    b. Entities with limited IT resources

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 will not 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. To Be Determined (TBD), but overseen by the IECC Finance Committee

12. **Who should be main lead of this deliverable?**
    a. IECC Member Jay Hochstetler

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?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Revise & circulate "Top Information Security Tips" to IECC for mass distribution | Jay Hochstetler | 25% | December 2022 | Review of original information with notes and additional content added. |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| 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.)**

a. None

| 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. 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. Better end-user information security posture, education, awareness, reporting, and response.

**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?**

☐No ☒ Yes

a. 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?**

☒No ☐ 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?**

☒No ☐ Yes

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

a. Periodic review by several resources (i.e. team members) to ensure content is relevant and updated.

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

a. The deliverable will be circulated internally to the committee to distribute as deemed necessary. This could include posting on a state website.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. Information security best practices are not industry specific.

## Communications

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

a. 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)?**

☐No ☒ 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 review and distribute the Top Information Security Tips 2.0 training material for Indiana businesses by December 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

# Supporting Documentation

# Supporting Documentation

- Top Security Tips Material 1.0

# IECC Finance Committee
# Top Security Tips Material 1.0

# Information Security Tips - 2019

# Harden Interior/Exterior

- Assess risk based on current threat environment and impact.
- Limit externally facing access to data.
  - VPN, email, servers, etc. Enable two-factor authentication (2FA).
- Limit ingress/egress points. Control local network access. Network segmentation.
- Change detection for new open ports, regular automated vulnerability scans.
- Enable host-based firewalls.
  - Do workstations need to talk to each other?
- Enable 802.1x.

# Proxy Traffic

- Implement network traffic filters.
- Intrusion Detection / Intrusion Prevention (internal & external).
- Full packet capture and net flow data is a necessity to determine if an incident occurred and what / how much data was transmitted.
- Don’t forget about SSL/TLS.
  - Where is your network packet visibility limited?
- Data Loss Prevention.
  - USB/CD blocking, webmail, email alerts.

# Know Where Your Data Lives

- Cloud, onsite, ancillary accounts for business purposes? Does your data auto-sync?
- 2FA wherever possible.
- Strong & unique passwords.
  - Password managers.
- If it doesn’t need to be stored online, don’t.

# Disable/Control Ancillary Services

- Services/applications that could be used in an attack. How are attacks occurring? Can we mitigate/prevent?
- Severely limit PowerShell, cmd, etc.
  - Enable PowerShell logging and alerting.
- Use Software Restriction Policies & Group Policies to your advantage.

# Group Policy

- Turn off access to USB/CD.
- Limit number of cached logons and don’t let wdigest store passwords in clear text.
- Harden UNC paths.
- Disable/severely limit macros in Office products and other commonly used scripting attacks methods.
- Block scripting in PDFs.

# Control Authentication

- Service / local account password randomization and very complex.
- User passwords with complex 12+ characters. Admins 15+.
- Disable WPAD.
- Enable SMB signing.
- Disable NetBIOS & LLMNR.
- Limit admin accounts.  Many current threats can execute as standard user.

# Control Authentication

- Vendor Accounts
  - How do they have access to your network?
    - Site-to-site VPN / Remote access VPN?
  - Principle of Least Privilege.
  - Disable when not in use.
- Very few admins need Domain Admin.

# Examine Phishing Attempts

- They are letting you know how they are trying to attack you, why just delete that message.
- NOT advisable to do this on your corporate network.
- Dedicated phishing email account and virus network/VM for testing user submissions.
- Have the ability to post process internal corporate network traffic.
- Train users on current phishing/social engineering trends.
- Enable DMARC and SPF inspection.

# Watch/Archive Logs

- Setup thresholds to auto email when anomalies are detected.
- In addition to the obvious failed logons and other potential indicators of compromise, set thresholds for too many successful logon attempts from one account.
  - Why did one user just log onto 100 machines successfully?
  - What other ways can you detect an attacker’s lateral movements?
- Set useful and relevant retention periods for logs.

# Control Mobile Users

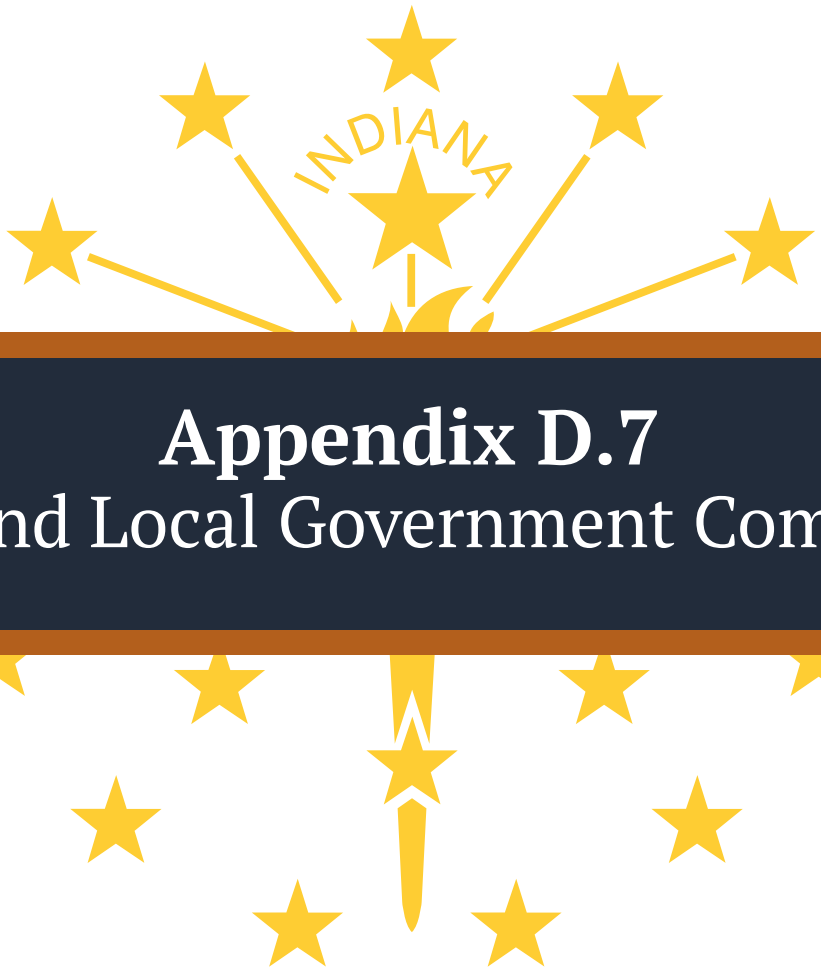
- Force VPN when off the network for mobile users. 2FA.
  - Built into most VPN applications.
- We want to have visibility into our machines, no matter their physical location.
- Encrypt all devices.

# Patch & Assess

- Set schedules, as often as possible.  Patch and assess your environment via vulnerability scanning to ensure patches are being deployed.
  - Nessus, Qualys, OpenVAS, etc.
- Respond to the vulnerability scan results.
  - What is not getting patched? If it can’t be patched, document why and implement mitigating controls.
  - If necessary, establish a manual patching process.

# Backups

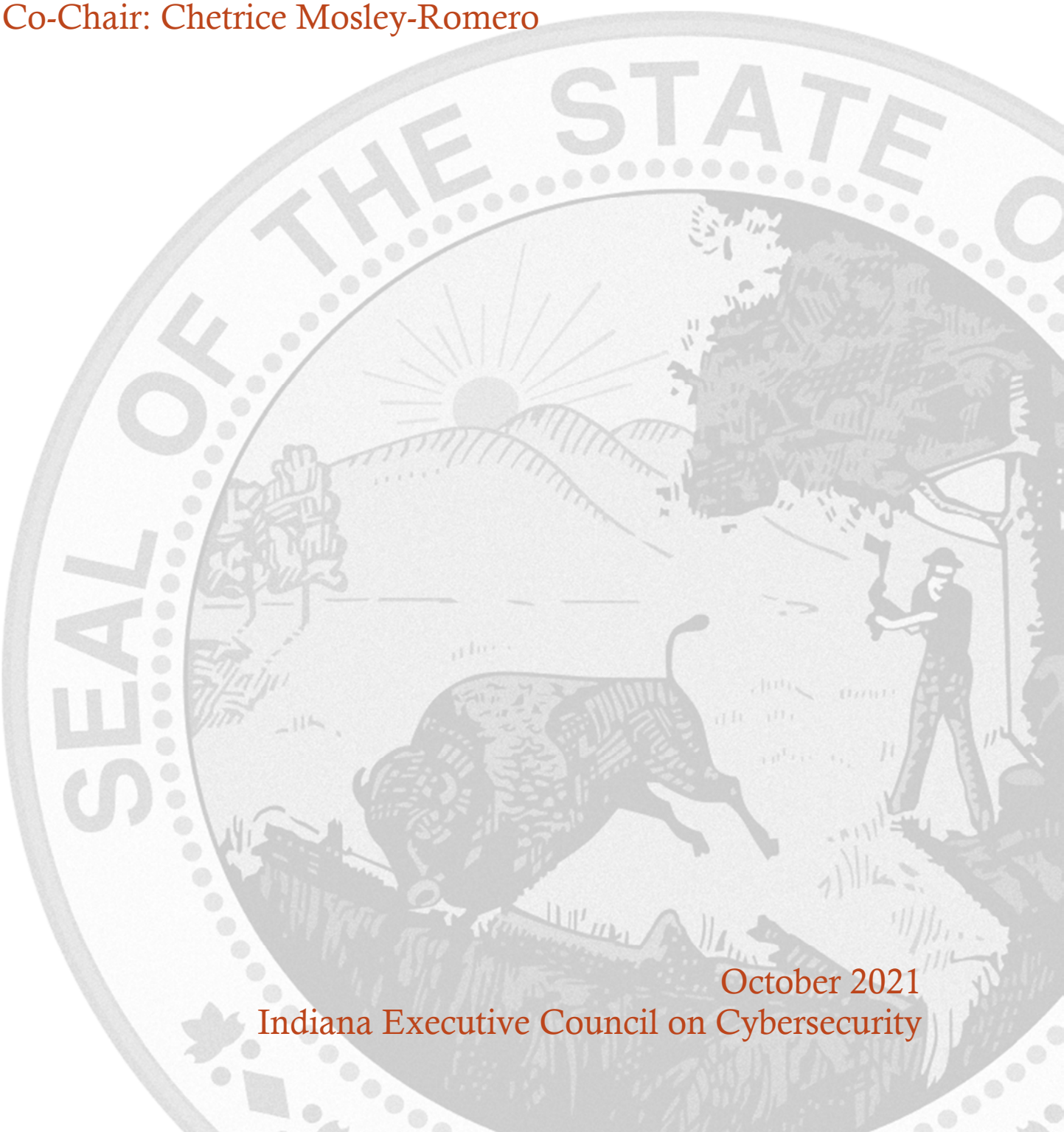
- Are they stored for long enough?
- Restore testing.
- Is your tertiary backup system online, on the same domain as your primary, use the same backup software?
  - Air-gap your backups.
- Data retention policy?




# Appendix D.7
## State and Local Government Committee

# STATE AND LOCAL GOVERNMENT COMMITTEE STRATEGIC PLAN

Chair: Stephanie Yager
Co-Chair: Chetrice Mosley-Romero



October 2021
Indiana Executive Council on Cybersecurity

# State and Local Government Committee Strategic Plan

# Table of Contents

# Committee Members

# Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Beckman | Joe | Purdue Technical Assistance Program | Managing Advisor - Security | Chair Proxy |
| Berry | Tim | Crowe, LLP | Managing Director | Full Time |
| Brown | James | Dark Chariot Consulting | CEO/Owner | Full Time |
| Carroll | Alex | Lifeline Datacenters | Principal | As Needed |
| Carter | Douglas | Indiana State Police | Superintendent | As Needed |
| Chari | Bharath | Deloitte | Cyber Risk Services | Full Time |
| Chu | Tony | Indiana Department of Revenue | Chief Information Security Officer | As Needed |
| Cook | Rhonda | Accelerate Indiana Municipalities | Deputy Director | Full Time |
| Driskell | Debbie | Indiana Township Association | Executive Director | Full Time |
| Ferdon | Mary | City of Columbus | Executive Director Administration and Community Development | Full Time |
| Gregg | John | Accelerate Indiana Municipalities | Grassroots Legislative Advocate | As Needed |
| Grennes | Bob | Indiana Department of Revenue | Commissioner | As Needed |
| Harper | Bryan | Indiana State Police | Criminal Investigation | Full Time |
| Jain | Hemant | Indiana Office of Technology | Chief Information Security Officer | Full Time |
| Johns | Jason | Sondhi Solutions | President | As Needed |

| | | | | |
|---|---|---|---|---|
| King | Brad | Indiana Election Commission | Election Division Co-Director | As Needed |
| Kroft | Kent | Tippecanoe County | Chief Information Officer | As Needed |
| Lohrentz | John | Munster Police Department | Intelligence Analyst / Digital Forensic Analyst | Full Time |
| Mertens | Chris | Hamilton County | Director of Information Technology | Full Time |
| Mitchell | Kelly | State Treasurer | Treasurer | As Needed |
| Poliquin | Daniel | Deloitte | Cyber Risk Services | Full Time |
| Renick | Timothy | City of Carmel | Director of Information and Communications Services | As Needed |
| Swetnam | Douglas | Indiana Office of Attorney General | Section Chief – Data Privacy and Identity Theft Unit | Full Time |
| Taylor | Nick | Netlogx | Chief Information Security Officer | As Needed |
| Turner | Larry | Indiana State Police | Lt. Colonel, Office of the Assistant Superintendent | As Needed |
| Wuellner | Mark | Indiana Bond Bank | Executive Director | Full Time |
| Yager | Stephanie | Indiana Association of County Commissioners | Executive Director | Chair |
| Giles | Clark | City of Indianapolis | Chief Technical Officer | Full Time |
| Stahl | Tad | IN-ISAC / Indiana Intelligence Fusion Center | Director / Deputy Director for Cyber Intelligence | Full Time |
| Byers | Bryan | Ball State University VSTOP | Co-Director, State of Indiana Voting Systems Technical Oversight Program (VSTOP), Professor of Criminal Justice and Criminology | As Needed |

| | | | | |
|---|---|---|---|---|
| Brown | Allen | Midwest Natural Gas | IT Director | As Needed |
| Heir | Rajinder | Indiana Commission for Higher Education | Chief Technology Officer | Full Time |
| Mosley-Romero | Chetrice | State of Indiana | Program Director | Co-Chair |
| Roeder | John | Lt. Governor's Office | Director of Legislative Affairs & Parliamentarian | As Needed |
| Shackelford | Scott | Program Chair and Director | Indiana University | As Needed |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan.*

For more information, visit www.in.gov/cybersecurity.

# Executive Summary

# Executive Summary

- **Research Conducted**
    - National Institute of Standards and Technology (NIST) Standards and Roadmap
    - 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
    - Information Sharing and Analysis Center (ISAC) – State Comparison Research
    - Multi-State Information Sharing and Analysis Center (MS-ISAC) documents and resources
    - U.S. Computer Emergency Readiness Team (US-CERT) documents and resources
    - Collection of Indiana State Agency Cybersecurity and Identity Protection Resources (In Process)
    - Local government partners also met periodically over the course of the last several years 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.

- **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.
- 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

- **2021 Committee Deliverables**
    - Indiana's Cybersecurity Hub Website
    - Indiana Cyber Emergency Resiliency and Response State Guide
    - Local Officials Cybersecurity Guidebook 2.0
    - Local Government Cyber Engagement Program
    - Identity Theft State Roundtable

- **Additional Notes**
    - The State and Local Government Committee is also working closely with the National Governors Association on its Local Government Cyber Engagement Program via their policy academy (See supporting documentation for proposal sent to NGA from the Governor).

# Research

# Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Indiana State Police (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. Indiana Department of Homeland Security (IDHS) – yber annex and Coordinated 16.1 and 16.2 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. State of Indiana Office of Technology (IOT): There are several initiatives that IOT has led or been very involved with since 2015 around the topic of cybersecurity.
        i. Indiana established a central information technology office in 2005 under an executive order by former Gov. Mitch Daniels and codified by the legislature that same year. Security was a focus from day one. The Office of Technology (IOT) has been tasked with reviewing, among other things, projects architecture and security. The state appointed its first chief information security officer (CISO) shortly after creating IOT.
        ii. The State initially focused on protecting agency applications, websites and developed policies and standardized fundamental security practices such as end-point protection, network segmentation, penetration process and risk assessments.
        iii. IOT, Purdue University, Cisco, FireEye & RSA partnered to create the Indiana Information Sharing & Analysis Center (IN-ISAC) in 2015. The IN-ISAC provides real-time network monitoring, vulnerability identification and threat warnings.
        iv. In 2016, the State of Indiana organized and participated in a critical infrastructure readiness and resiliency exercise utilizing an Indiana National Guard facility. The simulated cyberattack used a utility SCADA system housed on a separate grid, which allowed real attacks and results to occur. A variety of utility personnel manned the SCADA system while attacks occurred to see how they would respond.
        v. Indiana expanded its cybersecurity program through Executive Order 17-11, signed by Gov. Eric Holcomb in 2017. It is recognized nationally and led by the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana State Police, and the Indiana National Guard and the Indiana Executive Council on Cybersecurity (IECC). Recognized for its unique

structure, the membership of the Council is comprised of government officials (local, state, and federal), as well as stakeholders and experts from the private-sector, military, research, and the academic community.

vi. Indiana's cybersecurity program is centered on proactively providing guidance and resources to all Hoosiers, including units of local governments, businesses across a wide range of industries and markets, as well as to our K-12 schools, colleges, and universities.

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.
g. 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. Year-over-year, sophistication increases in phishing attacks. There is always an opportunity to refresh training and reinforce strong security awareness.
b. External threats, malicious insiders, employees who fall for social engineering schemes, and sensitive data outside of the State's protected zone.
c. For local governments it is typically emergency services, record keeping, water and sewer operations.
d. Employees and contractors, the human element, remain the greatest vulnerability to the State of Indiana. The number one weakness is staff clicking on a link opening an attachment or inadvertently releasing credentials that allow an attacker an entry vector.

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

a. The State of Indiana has a robust cybersecurity training program required of all employees and contractors. This monthly training is built on a variety of learning materials and builds upon each other, as well as reviews concepts. Despite the success of this program, cybersecurity defense requires 100% success. Any mistake or erroneous click can open the network allowing an attacker to slip in.
b. Continued partnership among public and private sector actors responsible for cybersecurity and cyber emergency response.
c. Coordination of messaging to private sector and local government related to available government services at the federal and state levels.
d. 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.
e. IDOR: Funding and manpower to support security assessments and implementation of security enhancements.
f. Additional resources and funding.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. The State of Indiana must follow federal compliance laws in cybersecurity, especially in areas of health and human services and taxes. The State has developed cybersecurity regulations that are created and managed by the Indiana Office of Technology. These policies are applicable to all state agencies.
    b. 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.
    c. 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.
    d. Local units' emergency management plans are subject to approval by the Indiana Department of Homeland Security.
    e. Public record keeping and retention schedules are governed by state statute under the guidance of the Commission on Public Records.
    f. 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. 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.
    d. 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. NIST Standards and Roadmap
    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
    l. ISAC – State Comparison Research
    m. MS-ISAC documents and resources
    n. US CERT documents and resources
    o. Collection of Indiana State Agency Cybersecurity and Identity Protection Resources (In Process)

p. The deliverables were based on the knowledge and expertise of the members serving on the Local Government Working Group.
q. Some resources that were cited and referred to over the course of our discussion include:
    i. The Indiana Local Government Technology Association
    ii. National Network of Fusion Centers
    iii. MS-ISAC - Multi-state Information Sharing Analysis Center
    iv. NIST Cybersecurity Framework paper

**7. What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**

a. See previous question.
b. Other States are also investing in employee and contractor training around cybersecurity, promoting a culture around shared responsibility and risk mitigation helps drive towards desired behavior. Phishing simulations, tabletop exercises are two examples of educating and preparing for an attack.
c. 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.
d. 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. Cybersecurity success is not a one and done event. There is no checking of the box to indicate we are done. This is an ongoing effort to continue to implement best in class support around our people, process and technology. Metrics can help drive towards increased adoption of cybersecurity policies, better phishing simulation results, and increased business enablement while operating within our risk appetite.
b. Implement 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. Update 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.
f. Overall, 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. The State of Indiana has a robust training program for state employees and contractors.
    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. 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.
    d. 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. Many state agencies have cybersecurity-related workforce.
    b. 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. The State of Indiana has developed an Incident Response Plan and offers additional resources to assess cybersecurity preparedness, including the Indiana Cybersecurity Scorecard. Developed by the State of Indiana and Purdue University, this 22-question tool will provide a score of where an organization stands in cybersecurity with easy-to-understand questions.
    b. 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.
    c. IDOR: We communicate based on our formalized process of identifying, analyzing, responding to, and recovering from incidents to include cyber emergencies
    d. 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. NIST Framework and Roadmap
    b. The state requires each of its vendors to follow best practices and strict guidelines. Indiana's cybersecurity strategy relies on a common-sense approach and encourages those entities who partner with us to utilize the best practices and industry standards, as defined by NIST and other accepted guidance as provided by USDHS, CISA and FEMA, among others.

c. The cybersecurity posture for the State of Indiana is supported by several principles outlined by Governor Holcomb through the Executive Order 17-11 and proclamation Gov. Holcomb issues the State of Indiana observes October as Cybersecurity Awareness Month.
d. 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.
e. 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: Indiana's Cybersecurity Hub Website

# Deliverable: Indiana's Cybersecurity Hub Website - Update

## *General Information*

1. **What is the deliverable?**
    a. Improve the Cybersecurity website (www.in.gov/cybersecurity) as the central hub for cybersecurity information in Indiana

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?**
☐ 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?**
☐ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

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. 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. Cyber Awareness and Sharing Working Group and 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. IOT will host the cybersecurity hub website and assist in revamping it. Other state agencies and federal agencies will review the resources and provide links to cybersecurity information.

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

a. Cybersecurity Program Director

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

a. Incorporating all the resources from state and federal agencies as well as public, private, and academic appropriately.

## *Implementation Plan*

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

☐ One-time deliverable

☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review website content | Cybersecurity Program Director, Cybersecurity Program Communications Manager, and IECC | 0 | February 2022 | |
| Make all minor website changes | Cybersecurity Program Communications Manager, | 0 | March 2022 | |
| Update website features and any large changes | Cybersecurity Program Director, Cybersecurity Program Communications Manager, IN.gov | 0 | June 2022 | |
| Test website and make edits | Cybersecurity Program Director and content team | 0 | July 2022 | |
| Website launches | IN.gov | 0 | August 2022 | |
| Present to IECC | IECC | 0 | Fall 2022 | |
| Implement Communications Plan | Cybersecurity Program Director | 0 | Fall 2022 | |
| Track stats | Cybersecurity Program Communications Manager | 0 | Every quarter | |
| Review and make additional edits annually | Cybersecurity Program Director, Cybersecurity Program Communications Manager, and IECC | 0 | September of every year | |

## 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 FTE | 1 FTE | Communications /Web master | State of Indiana | N/A | |
| 1 FTE | 0 | Communications and/or cybersecurity | State of Indiana | 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 |
|---|---|---|---|---|---|---|
| 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 continue to 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 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. ☐No ☒ Yes
   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. ☐No ☒ Yes

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?**

☒No ☐ Yes

**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. ☐No ☒ Yes

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)?**

☐No ☒ 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 conduct a major review and update of the Cyber Hub website by August 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

**Objective 2:** Increase website traffic to www.in.gov/cyber by 100 percent by September 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

**Objective 3:** Conduct an annual review and update the Cyber Hub website by September of every year.

*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 Resiliency and Response State Guide 2.0

# Deliverable: Cyber Emergency Resiliency and Response State Guide – Update

## *General Information*

1. **What is the deliverable?**
    a. Indiana Cyber Emergency Resiliency and Response State Guide – Update

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?**

☐ 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 Emergency Resiliency and Response State Guide was created to formalize partnerships and processes to be used to communicate to stakeholders during a cyber incident.

6. **What metric or measurement will be used to define success?**
    a. Completion of plan and distribution to appropriate partners and public.

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

☐ 2021 ☐ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

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. 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. Resiliency and Response Working Group and cyber awareness and sharing 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. State and Local Government 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?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Provide 2019 version of Indiana Cyber Emergency Resiliency and Response State Guide to Committee for review | Cybersecurity Program Director | 0% | January 2023 | |
| Edit Plan | Cybersecurity Program Director | 0% | March 2023 | |
| Review with IECC leadership | IOT, IDHS, INNG, ISP, Governor's Office | 0% | May 2023 | |
| Finalize Plan | Cybersecurity Program Director | 0% | July 2023 | |
| Distribute Plan | Cybersecurity Program Director | 0% | August 2023 | |

## 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 |
|---|---|---|---|---|---|
| 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 |
|---|---|---|---|---|---|---|
| No Response | | | | | | |

## 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?**

☐No ☒ Yes

a. There are other states that do have a disruption plan. The National Governor's Association has a list.

**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?**

☐No ☒ Yes

a. The states that are not listed to have this type of plan and the possible issues that have come from that may be a good indicator of the importance of this document.

## 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?**

☒No ☐ Yes

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

a. A point of contact must keep an eye on this document and update it if there are significant changes to the state's involvement and response capabilities during a cyber emergency and/or incident.

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

a. No Response

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

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. It was noted in the 2021 INCyber USDHS CISA that the state needs to do better at communicating about these types of guides to local emergency managers. In the development of the public relations plan and distribution, it would be important to work closely with IDHS in distributing it to them.

## *Evaluation Methodology*

**Objective 1:** The State of Indiana will update and distribute the Indiana Cyber Emergency Resiliency and Response State Guide by October 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

# Deliverable: Local Officials Cybersecurity Guidebook 2.0

# Deliverable: Local Officials Cybersecurity Guidebook 2.0 – Update

## *General Information*

1. **What is the deliverable?**
    a. The group's deliverable is an update to the 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?**

☐ Completed ☒ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

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. To continue 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 from local governments.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☐ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

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. There are many local government resources and programs that can be used to help develop this product.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All the committees have deliverables or resources that can be included

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?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Using lessons learned from the Local Government Cyber Engagement Project, review and edit the guidebook 1.0 for local officials | State and Local Government Committee | 25 | September 2022 | |
| Edit Guidebook | Cybersecurity Program communications manager and Purdue Partnership | 0 | January 2023 | |
| Finalize with Committee | State and Local Government Committee | 0 | March 2023 | |
| Launch guidebook | Cybersecurity Program Director and Cybersecurity Program communications manager | 0 | April 2023 | |
| Implement communications strategy around guidebook | State and Local Government Committee and IECC partners | 0 | May 2023 | |
| Track downloads from cyber hub website | Cybersecurity Program communications manager | 0 | Quarterly | Goal: 1,000 downloads in one year |
| Review and make needed edits to ensure accuracy of guidebook | Cybersecurity Program communications manager | 0 | Annually | |

## 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 |
|---|---|---|---|---|---|
| 1.5 FTE | N/A | Technical writer/editor | State of Indiana | Grant or contribution | |

**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 |
|---|---|---|---|---|---|---|
| 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. The Guidebook will provide the information needed to assist local government units with drafting their own cybersecurity plans, which plans would provide instruction and guidance to prevent and mitigate cybersecurity attacks.
b. 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. This could cause disinformation or put in place bad processes that could hurt local governments. Even if correct information or good processes are implemented, the time it will take for a local government not versed in cybersecurity to find and vet information is a cost of person-hours and resources. The Guidebook will avoid reinventing the wheel by providing trusted resources, known to work.

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

a. The completion and distribution of the guidebook.

**21. 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

i. Aware of other states such as West Virginia and Michigan who have done campaigns and projects with local government, in addition to providing guidance.

**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?**

☐No ☒ Yes

i. There are many states who have not done much outreach to local governments regarding cybersecurity.

## Other Implementation Factors

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

a. Not enough time and resources to edit guidebook.

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

☒No ☐ Yes

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

a. As new information evolves, it is foreseeable that the guidebook will require updating and reposting.

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

a. IOT, Indiana Financial Authority (IFA), IECC Water/Wastewater Committee, Legal/Insurance Working Group.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

i. The best practices for cybersecurity 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)?**

☐No ☒ Yes

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

a. It is imperative to work closely with the associations to get the word out about the guidebook, as they are trusted advisors to the local units. In addition, showcasing the guidebook in workshops and educational events at conferences will be important as well in getting the word out with local governments. Many units of government work with professionals who specialize in municipal work; identifying those trusted professionals and providing them the resource for distribution to their municipal client base as a value-add service could be another delivery mechanism. Similarly, identifying state agencies that work with local units of government as trusted partners and asking they make available or push out the Guidebook could assist in the uptake.

## *Evaluation Methodology*

**Objective 1:** The State and Local Government Committee will update and distribute the Indiana Local Government Cyber Guidebook by May 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

**Objective 2:** The State and Local Government Committee will encourage the downloading of 1,000 Indiana Local Government Cyber Guidebooks by May 2024.

*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: Local Government Cyber Engagement Program

# Deliverable: Local Government Cyber Engagement Program

## *General Information*

1. **What is the deliverable?**
    a. Local Government Cyber Engagement Program

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?**
    ☐ 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 of the local government cyber engagement program is to empower local governments with the tools and practices to increase their cybersecurity posture.

6. **What metric or measurement will be used to define success?**
    a. Using the developed program, pilot it with 5-7 local governments and they provide the State with feedback of how we can better provide support where appropriate.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☒ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Local governments (townships, cities, municipalities, and counties)

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. There are several resources we are looking to assist with this program, especially with USDHS.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The committee will be interfacing with the entire IECC and all the committee and working groups to complete the program.

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. Several federal and state agencies that work directly with local government will be involved.

12. **Who should be main lead of this deliverable?**
    a. Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. Limited time and resources for the local governments, state, and federal agencies, as well as the many private and academic organizations who will be assisting with this program.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Developed outline of idea and receive approval by State cyber leadership and Governor's office for NGA policy academy | Cybersecurity Program Director | 100 | March 2021 | |
| Was selected by the NGA academy for project | Cybersecurity Program Director | 100 | April 2021 | |
| Began working through the outline of the program with committee | State and Local Government Committee and IECC | 100 | May 2021 | |
| Draft outline and collect materials for program matrix | Cybersecurity Program Director, State and Local Government Committee, NGA | 50% | June – December 2021 | |
| Select participants for pilot of program | Cybersecurity Program Director, State and Local Government Committee | 75% | October 2021 | |
| Hold virtual workshop (hosted by NGA) to:<br>a. finalize the program matrix<br>b. define the matches of functions of local government to the source materials for the program<br>c. determine the most effective way to engage local govt. pilot participants and steps forward | Cybersecurity Program Director, State and Local Government Committee, NGA | 0% | November 2021 | |
| Using what is learned from the virtual workshop work to:<br>a. Pare down the functions<br>b. Plan to give products to locals, matching functionality to level to resources<br>c. Workshop template plan, POCs, assignments, etc.<br>d. Communicate plan to the locals<br>e. Gather materials, information and resources | Cybersecurity Program Director, State and Local Government Committee, Academic partners, NGA | 0% | January 2021 | |

| | | | | |
|---|---|---|---|---|
| f. Develop launch and support documents<br>g. Match functions with IECC mentors | | | | |
| Launch program with pilot groups Indiana – In-person workshops | Cybersecurity Program Director, State and Local Government Committee, Academic partners, NGA | 0% | February/March 2022 | |
| Work with each pilot program and do regular check ins | Cybersecurity Program Director, State and Local Government Committee, Academic partners | 0% | Monthly for six months from launch | |
| Conduct 6-month presentation workshop | Cybersecurity Program Director, State and Local Government Committee, Academic partners | 0% | August/September 2022 | |
| Do annual presentation workshop/final check-in | Cybersecurity Program Director, State and Local Government Committee, Academic partners | 0% | February/March 2023 | |
| Using the lessons learned from the pilot group, make adjustments to program and get it ready for a full-state launch | Cybersecurity Program Director, State and Local Government Committee, Academic partners | 0% | December 2022 | |
| Develop a communications plan to launch to full state | Cybersecurity Program Communications Manager | 0% | December 2022 | |
| Launch the program to all local governments to self-guide and use | Cybersecurity Program Director, State and Local Government Committee, | 0% | January 2023 | |

| | | | | |
|---|---|---|---|---|
| | Academic partners, all IECC | | | |
| Track number of participants | Cybersecurity Program Communications Manager | 0% | Quarterly and annually | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

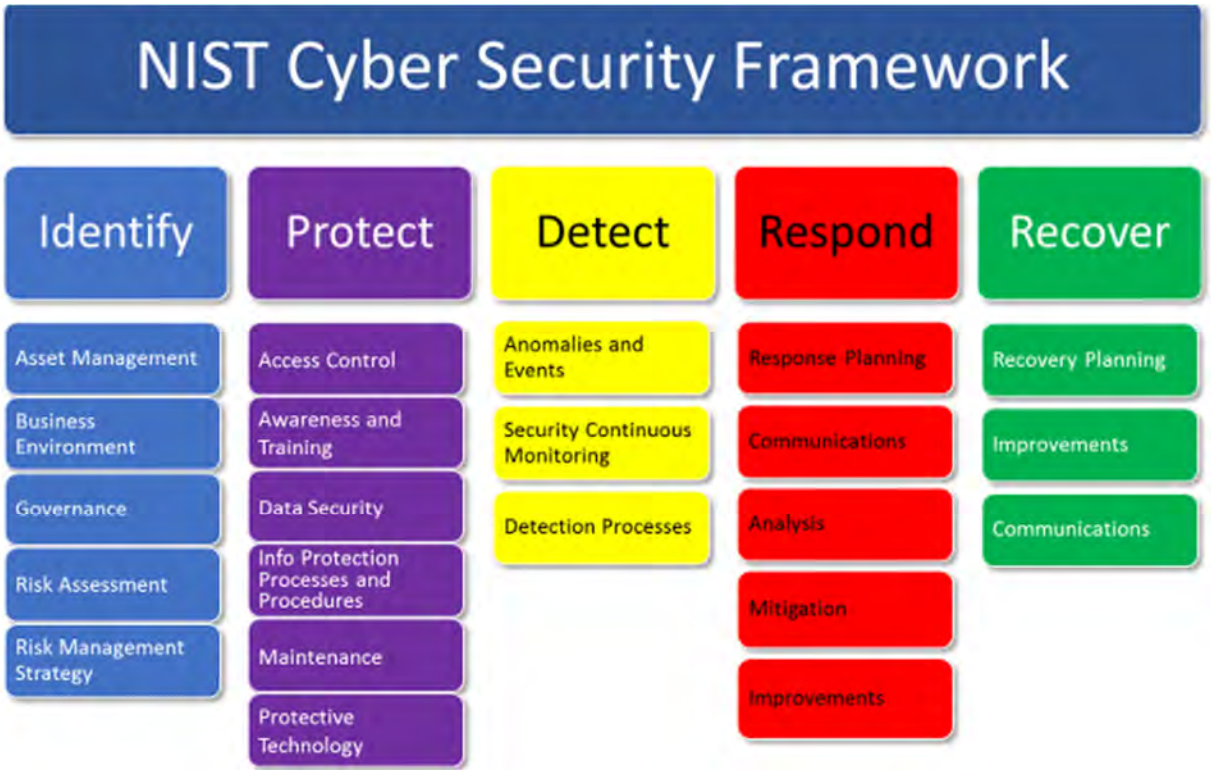
☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 3.5 FTE | 2 | Managing resources for local governments along with state and federal throughout the program | State of Indiana – IOT/IDHS (IECC Support) and IN-ISAC | N/A | Indiana ISAC may be a better source of management long-term once the IECC staff has developed and piloted the program. |

**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 |
|---|---|---|---|---|---|---|
| Identify resources | See below image for the types of services we may need to consider in this project. | N/A | N/A | N/A | N/A | |
| Protect resources | See below image for the types of services we may need to consider in this project. | N/A | N/A | N/A | N/A | |
| Detect resources | See below image for the types of services we may need to consider in this project. | N/A | N/A | N/A | N/A | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Respond Resources | See below image for the types of services we may need to consider in this project. | N/A | N/A | N/A | N/A | |
| Recover Resources | See below image for the types of services we may need to consider in this project. | N/A | N/A | N/A | N/A | |




## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. This deliverable will provide the local government the many resources that the IECC has developed and has collected in a way that is focused on operational function making the project of “increase your cybersecurity” more digestible and applicable for those who serve in local government.

18. **How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?**
    a. Developing this program and local governments using this program will make them more aware of their cybersecurity posture, be able to empower them with the steps to take with some guidance of priorities so that they are able to effectively 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 local government will continue to struggle with the variety of resources, oversaturation of information, and receiving different cyber efforts from the state which cause frustration and confusion. If they are not found, then local governments may find it more difficult to raise their cybersecurity level and more vulnerable to cyberattacks on our critical infrastructures.

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 a guide/matrix to guide the 5-7 local governments who will volunteer to pilot the program. After feedback is applied to the program, voluntary adoption of the program by 25 percent of Indiana local governments by 2025 will be the ultimate 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?**
    ☒No ☐ Yes

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?**
    ☐No ☒ Yes
    a. Many states have provided resources to local governments, but no state has created an comprehensive program

## Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. Scope of the project and volunteer time and financial resources my be factors that can negatively affect this deliverable.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. ☒No ☐ Yes

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. It will require a program manager.

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

a. Local governments, IECC committees/working groups, and NGA.

**27. Can this deliverable be used by other sectors?**

a. ☐No ☒ Yes,

i. All sectors can use the best practices and processes we will be developing with this program

## Communications

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

a. All IECC members and partners as well as all Indiana local governments

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

☐No ☒ Yes

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

a. None at this time. Will have more about other considerations after we have completed the pilot.

## *Evaluation Methodology*

**Objective 1:** The State and Local Government Committee with the assistance of IECC partners and the National Governors Association, will develop the Local Government Cyber Engagement Program by January 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

**Objective 2:** The State and Local Government Committee with the assistance of IECC partners and the National Governors Association, will pilot the Local Government Cyber Engagement Program with at least five local government entities by June 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

**Objective 3:** The State and Local Government Committee with the assistance of IECC partners will publicly launch the Local Government Cyber Engagement Program by January 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

**Objective 4:** As a result of outreach efforts, at least 30 local government entities will have begun using the Local Government Cyber Engagement Program 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

# Deliverable:
# State Agencies Roundtable: Identity Theft

# Deliverable: State Agencies Roundtable: Identity Theft

## *General Information*

1. **What is the deliverable?**
    a. State Agencies Roundtable: Identity Theft
    Using DWD's first-hand experiences related to hacking attempts, claim hijacking, and identity theft over the billions of dollars available in the federal relief for the unemployed, DWD and IOT will host a round-table discussion with other state agencies to share concerns and best practices that were encountered.

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?**
    ☐ 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 of the State Agencies Roundtable: Identity Theft is to open dialogue up of lessons learned and best practices between agencies with regard to protective measures against identity theft and fraud.

6. **What metric or measurement will be used to define success?**
    a. Have at least six key state agencies gather to openly discuss lessons learned and best practices between agencies with regard to protective measures against identity theft and fraud.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. Appropriate state agencies

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. There are a variety of resources around tax and unemployment fraud from other states and federal agencies to assist in the conversation of the round table.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Workforce Development Committee and Privacy 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, IDOR, DWD, BMV, and any other state agency that serve on the IECC.

12. **Who should be main lead of this deliverable?**
    a. State CIO and DWD Commissioner.

13. **What are the expected challenges to completing this deliverable?**
    a. Having the available time and resources to meet.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Initial Planning meeting | Cybersecurity Program Director with the State CIO and DWD Commissioner. | 0 | December 2021 | |

| | | | | |
|---|---|---|---|---|
| Develop invite list | Cybersecurity Program Communications Manager . | 0 | January 2022 | |
| Lock in room, logistics, and time | Cybersecurity Program Communications Manager | 0 | January 2022 | |
| Send invite | Cybersecurity Program Director with the State CIO and DWD Commissioner. | 0 | February 2022 | |
| Hold roundtable | Cybersecurity Program Director with the State CIO and DWD Commissioner. | 0 | May 2022 | |
| Develop memo to share with state leadership of the lessons and key takeaways of the roundtable | Cybersecurity Program Communications Manager | 0 | June 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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. Using DWD's first-hand experiences related to hacking attempts, claim hijacking, and identity theft over the billions of dollars available in the federal relief for the unemployed, DWD and IOT will host a round-table discussion with other state agencies to share concerns and best practices that were encountered.

**18. How will this deliverable reduce the cybersecurity risk or impact?**

a. What are the estimated costs associated with that risk reduction?
Through open discussion and sharing best practices, cyber risk could be lowered.

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

a. No Response

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

a. Good attendance of the agencies invited and good conversation during the roundtable.

**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 ☐ Yes

b. It would be surprising that no state has done this internally, but none that we are aware of at this time.

**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?**

☒No ☐ Yes

## 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 ☐ Yes

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

a. It does not require sustainability.

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

a. Workforce Development Committee

**27. Can this deliverable be used by other sectors?**

a. ☐No ☒ Yes,

i. Best practices can be noted an available to share with trusted sources.

## Communications

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

a. IECC members

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

☒No ☐ Yes

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

a. None at this time.

## *Evaluation Methodology*

**Objective 1:** Indiana Department of Workforce Development (DWD) and Indiana Office of Technology (IOT) will lead a round table discussion with other key state agencies about best practices with defending against identity theft and fraud.

*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: Local Government Cybersecurity Podcast Series ("Days of Our Cyber Lives")

# Deliverable: Local Government Cybersecurity Podcast Series ("Days of Our Cyber Lives")

## *General Information*

1. **What is the deliverable?**
    a. Local Government Cybersecurity Podcast Series ("Days of Our Cyber Lives")

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?**
☐ 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. This deliverable has multiple intended resulting actions: (i) provide timely and relevant cybersecurity content to local units of government, (ii) engage state government offices and agencies who are not cyber-focused but have strong connections with local units of government into the IECC work, (iii) prompt local units of government to engage with the IECC's cyber-content, including the Hub, and (iv) serve as a gateway to other cyber resources from the state.

6. **What metric or measurement will be used to define success?**
    a. Total listeners/viewers of podcast over one year podcast series >= 900 (aka 75 audience/month x 12 months)

7. **What year will the deliverable be completed?**
    ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. Local units of government statewide
    b. Professionals supporting local units of government
    c. State entities such as IECC and IOT to distribute their messages and resources
    d. General public listeners

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

## Additional Questions

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

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. Mark Wuellner, Executive Director, Indiana Bond Bank

13. **What are the expected challenges to completing this deliverable?**
    a. Minimal challenges outside of lining up podcast guests (low difficulty)

## *Implementation Plan*

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

    *Note: A bit of both – it's a one-time total deliverable distributed in 12+ ongoing episodes recorded and released over a one-year period*

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Record min. 12-episode podcast series over course of 1 calendar year | Wuellner | 100 | October 30, 2021 | *Actual Episodic log attached as "Exhibit A" |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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?**

a. Meets this committee's objective of delivering critical cybersecurity content, tips and tricks and creating awareness of the IECC and state resource hub without technical jargon.

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

a. All episodes will deliver actionable content for a local government to put into place, many of which will be no or low-cost tactics or tips. For local governments that follow through, their cybersecurity risk would be reduced.
b. Additionally, many of the episodes will redirect to linked content for resources relevant to that episode's content. For example, if cyber incident reporting is addressed, the podcast will be posted along with links to relevant reporting forms available on the hub.
c. Finally, the podcast creates a connection between state leaders on cybersecurity (IECC Program Director especially) and a key audience of local government leaders, who may see the state resources as human and available after listening to the podcast.

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

a. This Committee believes the delivery of cybersecurity information to local units of government must be a multi-channel, multi-messenger mode of delivery. It may take multiple receipt of the same information from a variety of trusted sources for a local unit to implement a message. Therefore, using every trusted connection to local government is key to pushing the messages out. We have and are doing that through our strong network of local trade associations. If we did not do this podcast, we would fail to use the platform with local governments that naturally exist between the Indiana Bond Bank, a state quasi-agency whose customers are local units of government, and the State Treasurer's Office, which is viewed as a thought leader for local governments on financial and investment issues (two areas of vulnerability for cyber incidents).

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

a. Total listeners/viewers of podcast over 1 year podcast series >= 900 (aka 75 audience/month x 12 months)
b. Baseline for choosing 75 combined views & listens is multiple: (i) new podcast series (ii) on a technical topic (iii) to a niche audience (iv) with an unknown level of familiarity with podcasts. Achieving 75/month in that environment would constitute 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?**

☒No ☐ Yes

**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?**

☒No ☐ Yes

a. While no other state appears to use a podcast to deliver cybersecurity information through trusted sources to local government units, there is no control. That is a status quo norm.

## Other Implementation Factors

---

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

a. Securing guests (not anticipated as difficult)
b. IBB's ability to process raw recording into final product (not anticipated as difficult)
c. Willingness of guests and IECC members to promote and share the podcast episodes through their channels (will vary; more sharing should increase likelihood of hitting the metrics)

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

☒No ☐ Yes

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

a. This is a one year, start to finish, deliverable. There is a possibility it could be revisited in a future year if a success, or if new content is available, or if demand exists.

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

a. Indiana Bond Bank and State Treasurer's Office contacted the committee proactively to offer to provide this deliverable.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes,

a. Any, general public. The content to be provided, while often specific to units of government, should be generally applicable, and the Cyber Hub resources likewise should be useful to many beyond this sector.

## Communications

---

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

a. The potential audience are informed throughout the cycle of the deliverable due to the episodic nature of it; minimum 12 touches per year.
b. Post-completion, IBB can continue to push out relevant episodes. For example, the Halloween themed episode in 2020 can be repromoted in 2021 so that a new audience can engage in the still-relevant content.

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

☐No ☒ Yes

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

a. The more marketing the better. No paid marketing need be used. This can be easily promoted via social media channels or included in relevant e-newsletters from Committee members.

## *Evaluation Methodology*

**Objective 1:** Completion of a minimum episode podcast series on cybersecurity topics for a Hoosier local unit of government audience over the course of one year, available via audio-only (e.g., Apple Podcasts) or video and audio (YouTube) by October 2021.

*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 podcast series draws greater than or equal to 900 combined views & listens for the series by October 2021.

*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.

- Local Government Guide 1.0
- NGA proposal package
- Podcast Statistics as of October 2021

# Local Government Guide 1.0

# Cybersecurity Guide to Planning & Evaluating Risks for Indiana Local Officials

March 2021

A publication made possible by the following associations:
Association of Indiana Counties
Accelerate Indiana Municipalities
Indiana Association of County Commissioners

*With technical assistance provided by Purdue University*

# TABLE OF CONTENTS

# I. INTRODUCTION

As local government functions have become more automated and computerized, the risk of cyberattacks has become more concerning. From providing emergency response through 911 call centers to safe drinking water through municipal water treatment plants, local governments in Indiana are charged with providing services that are critical to life and living for the general population. Imagine if these critical services were suddenly disrupted by a malicious act – a cyberattack.

A cyberattack can be mounted against digital devices. It is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyberattacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks. Depending on the intent of the attacker, a cyberattack can be merely a nuisance or it can be potentially life threatening.[1]

**ATTACKS ON GOVERNMENT IN INDIANA**

Unfortunately, several Indiana local governments have already fallen victim to cyberattacks. For instance, in 2019, LaPorte County government was forced to pay $132,000 to hackers after a ransomware cyberattack shut down part of the county's computer system.[2] In 2017, in Franklin County, the county's financial software vendor was hit by an attack, which then allowed the county's records to be affected. While the county lost the records of one day's work, other work was saved by virtue of a backup done the night before. The Franklin County Auditor and Treasurer disabled user rights to view information in the financial system as a result of the attack in order to protect the security of the records.[3] In Madison County, 2016, hackers launched a ransomware attack on 600 computers and 75 servers and forced law enforcement officers to use pen and paper when processing inmate information at the local jail. Officers on patrol had to contact other agencies in order access a person's criminal records. On the advice of its insurance carrier, county officials paid the $21,000 ransom. The county later approved spending nearly $200,000 to secure additional IT contracts which included off-site data storage, a backup court system and protections against future infections.[4]

Indiana state government fell victim to attack in 2018. Federal prosecutors issued indictments and financial sanctions against Iranian hackers that illegally accessed Indiana state government computers. The hackers also accessed the computer systems of 144 universities where they stole data and intellectual property across all fields of research including engineering, medicine, science and technology. The hackers pretended to be professors at other schools and sent emails to the victim professors expressing an interest in their academic articles. The emails included a link to other articles that required the victim professors to enter their login information. The hackers then captured the login credentials and used it to access the university computer systems.[5]

## WHY TARGET LOCAL GOVERNMENTS

While local governments may not seem like great targets because of the money or the data they collect, local governments are enticing targets to hackers because of their digital connections. Local government computers are digitally connected to state and federal computers. The hackers end goal is to access state and federal databases. While the federal databases have stronger security shields, it is not the same for other connected computers at lower levels of government. Rather than trying to hack straight into the federal system, an easier route might be to go through a local, more vulnerable, computer system that is digitally connected.[6]

There has been an increase in cyberattacks targeting state and local government organizations mainly because these levels of government have fewer resources than the federal government. A report released in late 2019 showed that at least 174 municipal organizations were targeted by ransomware in 2019 – a 60% increase over 2018.[7]

## STAY INFORMED AND BE PREPARED

For many people, they don't consider themselves to be Information Technology (IT) or computer savvy, however, because the threats are real and the services provided by locals are critical, all local officials and employees must take the cybersecurity problem seriously. To promote more awareness of the need for cybersecurity planning, the following organizations collaborated on this publication: the Association of Indiana Counties (AIC), Accelerate Indiana Municipalities (Aim), and the Indiana Association of County Commissioners (IACC) to provide an overview of the cybersecurity planning process.

## ACKNOWLEDGMENTS

The local government associations would like to thank Purdue University's Technical Assistance Program cyberTAP group, along with Mark Green and Jason Dell from Network Solutions, Inc., and Todd Vare of Barnes & Thornburg for their specific contributions to Part 3 of this publication.

# II. STATUS OF LOCAL GOVERNMENT

**AWARENESS**

While there is little quantifiable data available at the present about the preparedness of local governments in Indiana to guard against cyberattacks, on a nationwide basis, the International City/County Management Association notes that most local governments in the United States don't have a strong grasp of the policies and procedures they should implement to protect their technology systems from attacks.[8] Forty-four percent of local governments nationwide reported that they regularly face cyberattacks on either an hourly or daily basis. More troubling is the high percentage of governments that do not know how often they are attacked (28 percent) or breached (41 percent). Further, a majority of local governments nationwide do not catalog or count attacks (54 percent). [9]

**LOCAL GOVERNMENT RESOURCES**

In 2019, county governments in Indiana received a boost with their cybersecurity protection efforts. The Indiana Secretary of State's Office entered into an agreement with California-based FireEye Security to provide counties with desktop and email protection, as well as 24/7 live network monitoring. The effort initially focused on county clerk's offices and elections related personnel but broadened to include all end points. Using federal funds purposed for election security, the secretary of state provided FireEye's capabilities to all 92 counties at no cost for three years. Senate Enrolled Act 179 (Public Law 135) passed by the Indiana General Assembly in 2020 *required* counties to enter into an agreement with the Secretary of State to use the FireEye software for specified security purposes.

One thing that is apparent about local governments in general is that there is a varied level of resources available to devote to IT matters in general. While some larger counties may have 25 or more IT professionals[10], other units of local governments such as small towns may not even have outside IT assistance engaged year-round on a contract basis.

# III. INITIAL PLANNING FOR CYBERSECURITY

**WHERE DO WE START?**

Though cybersecurity is different from traditional risks facing local governments, it is fundamentally a risk management challenge centered on the protection of electronic information and systems. The U.S. government standard framework for managing information systems risk is detailed in a series of National Institute of Standards and Technology (NIST) Special Publications (SPs) shown in Figure 1, below.[11]


Figure 1: NIST Risk Management Framework

Section V of this guide describes the process for identifying and managing cybersecurity risk in terms of the NIST Risk Management Framework while providing guidance and resources targeted specifically at local governments.

**WHO SHOULD BE AT THE PLANNING TABLE**

In order to start the cybersecurity planning process, local leaders must create a culture of cybersecurity that imagines worst-case scenarios and explores a range of solutions to mitigate threats to the ecosystem of local government technology. This involves prioritizing funding for cybersecurity, establishing stronger cybersecurity policies and training employees in cybersecurity protocols. Cybersecurity is more than just the IT department's problem. Success will require collaboration with:

- Local elected officials
- Internet-technology and cybersecurity staff members

- Department managers
- End users[12]

**PLANNING TIME FRAME / WRITING THE PLAN**

Developing your cybersecurity plan is going to involve research and fact finding. Depending on the local unit of government's size, you can expect plan development to take between six months to one year, or longer. While developing a cybersecurity plan is discussed in greater depth under Section IV, it starts with risk assessment which includes knowing what assets you own and finding out what insurance companies will require in order to obtain an insurance policy. Once you have the results of your research regarding risk assessment, you will group your risks into like categories, address those groups as part of a cybersecurity plan, and develop a one to two year plan to address the following: realistic timelines and answers, internal project management and internal resources.[13]

Your plan will need to be written and communicated throughout your unit of government. It is recommended that the plan should include a one to two page executive summary with the main findings, a spreadsheet or table showing the initial plan, along with a 20-25 page document showing the security plan which details timelines, staff needed, money needed and estimated completion time for each item.[14]

Though this guide focuses on the security of electronic information and information systems, your government should ensure that risks related to paper records are categorized, assessed, controlled, and monitored as part of the same process used for electronic information and systems.

# IV. CREATING A CYBERSECURITY PLAN

The *state* governments that are currently leading in cybersecurity have adopted and implemented security controls based on nationally recognized frameworks. Two of the leading and most commonly adopted frameworks are the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the International Organization for Standardization.[15] Our recommendations here are based on the NIST Framework, which is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size. Because each organization's risks, priorities and systems are unique, the tools and methods used to achieve the outcomes described by the NIST Framework will vary. [16]

The NIST framework recommends a five step approach:

1) Identify
2) Protect
3) Detect
4) Respond
5) Recover

**IDENTIFY YOUR ASSETS / RISK MANAGEMENT**

First, a local unit of government must develop an understanding of their systems, people, assets, data, and capabilities.[17] At the top of the list is critical infrastructure. The US Patriot Act of 2001 defines "critical infrastructure" as "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." NIST recommends that due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing and managing cybersecurity risks. [18] This approach is necessary regardless of an organization's size, threat exposure, or cybersecurity sophistication today.[19]

Risk management is the ongoing process of identifying, assessing and responding to risk. With an understanding of risk tolerance, local governments can prioritize cybersecurity activities, enabling local officials and staff to make informed decisions about cybersecurity expenditures. A local unit may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.[20]

It is important that local units identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.[21] In addition, it is important for local units to embark on supply chain risk management (SCRM) during the procurement process because outside suppliers of goods and services can introduce vulnerabilities to the local unit's cybersecurity. The primary objective of

cyber SCRM is to identify, assess, and mitigate products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain. These activities may include determining cybersecurity requirements for suppliers, instituting the requirements through contracts or other formal agreements, communicating with suppliers how the cybersecurity requirements will be verified, and verifying and validating that the requirements have been met.[22]

**PROTECT YOUR ASSETS**

The second step is to protect your assets by developing and implementing appropriate safeguards to ensure delivery of critical services.[23] Protecting assets requires a multi-faceted approach. It includes identity management and access control, awareness and training, data security, information protection processes and procedures (such as backups and redundancies), maintenance, and using protective technologies (such as firewalls – software that prohibits suspicious information from delivery).[24]

**DETECT INCIDENTS**

Detection requires development and implementation of appropriate activities to identify the occurrence of a cybersecurity event.[25] Being able to recognize an anomaly or an event is key and this only occurs through continuous security monitoring and institution of detection processes.[26]

**RESPOND WITH A PLAN**

Investments in planning and exercises support timely response and recovery actions following the detection of a cybersecurity incident, resulting in reduced impact to the delivery of services.[27] It must be contemplated in advance what potential system failures might occur and what plan of action would take place based on each scenario. Prioritization of critical infrastructure and systems is important. For instance, if all systems went down within your local unit of government, it's likely that any support to emergency medical services or 911 would be at the top of the list to be restored.

Testing the viability of your plan is also important. Mock cyberattack exercises should be part of your response planning procedures.

**RECOVER NORMAL OPERATIONS**

Your end goal is to restore any capabilities or services that were impaired due to a cybersecurity incident.[28] Once operations have been restored, it is important to go back and review the incident to analyze the effectiveness of the response and timing.

# V. CYBERSECURITY AS RISK MANAGEMENT

**CATEGORIZING INFORMATION SYSTEMS**

The goal of categorizing of information and systems is to determine the severity of the impact to your government and its citizens if the *confidentiality, integrity, or availability (CIA)* of the information, or the systems affecting that information, is impaired. Information and systems impact categorization is a crucial first step in the development of your information security plan because these categorizations drive the types and amount of controls used to safeguard the information that your government owns and manages. If too little control is applied to information, your government will face an unacceptable level of information security and privacy risk. If high impact controls are applied to all of your government's information, unacceptable levels of cost will result. So, organizations first need to inventory and categorize information and systems before they can properly apply controls to those data and systems.

In some cases, information risk categorizations are made for your government through regulation. For example, loss of CIA of health information regulated by the HIPAA Security and Privacy Rules is considered high impact because of the ramifications defined in regulation. In other cases, impact categorization is more nuanced. While building plans may not create a high impact of CIA if compromised in most cases, loss of confidentiality of the plans to the county jail or a chemical treatment plant could create a severe, negative impact on several local governments and populations. Emergency dispatch information may not be confidential, but is high-impact data because its availability is critical to the safety and security of your citizens. If your government is new to information impact categorization, or to cybersecurity planning more broadly, you should begin with broad categorizations. As the cybersecurity maturity of your government increases, your categorizations should become more nuanced. Developing more nuanced information impact categorizations is one reason why cybersecurity maturity and planning is an iterative process that requires constant effort.

**SELECTING SECURITY CONTROLS**

Well-designed security controls provide a level of security and privacy protections to information that match the impact categorizations through a wide range of threats to your environment with minimal impact on the function of the system or information. Because information is increasingly stored and transmitted electronically on systems administered by information technology professionals, controls applied to these data are often technical. However, the most effective controls regimes incorporate physical and administrative controls, as well as technical. For example, preventing malicious actors and/or software from accessing an e-mail system requires technical controls that stop known malicious software types and e-mail from known malicious addresses. But, e-mail security improves when users are required by policy to use strong passwords, change those passwords regularly, and are trained to recognize and respond to phishing e-mail messages that find their way through technical defenses. Layering multiple controls against information security threats is known as "defense in depth" and is the most

effective and resilient way to protect information and information systems. Several resources including: policy templates, controls frameworks, and technical guidance for your systems can help your government select the best controls for your particular environment.

**IMPLEMENTING SECURITY CONTROLS**

Because information security controls may be administrative, technical, and physical controls in nature, and because all local government employees have more access to the information and systems of their government than regular citizens, *all members of your organization have a role in implementing effective information security controls*. A key information security control is the use of unique access credentials for each individual user. In order to effectively implement this control, human resources or departmental personnel must notify an IT administrator to add a new, unique user to systems impacted by the hire. The IT administrator must add the new user and properly configure the new user's account, and most importantly, all users must keep their credentials secret and unique to themselves. Even when information security controls are limited to specific departments or functions, such as data backups or policies related to specific regulations like HIPAA, multiple people are involved. Therefore, all controls should be well documented and training should be developed that addresses each control and the reason for its use.

Organizational leaders have special roles in implementing information security controls. Once controls are selected, and associated policies and procedures developed are approved, leaders must consistently enforce policies and procedures. Doing so, along with constantly explaining and advocating for the use of the information security-related controls, builds a culture of information security that is a critical component of successful and mature information security programs. Most importantly, leaders must always abide by information security controls that are put in place for their organizations. While cases exist where the application of controls will necessarily differ among groups within your government, these cases must be documented and approved prior to their implementation and should be as close to the standard implementation of the control as possible.

In addition to documentation, training, and enforcement through leadership, successful implementation of controls requires that controls effectiveness be monitored. If, for example, a new acceptable systems use policy is implemented, requiring members of the organization to sign the policy provides a monitoring point that can be used to signify that users have read and understand the policy. If "acceptable systems use" in your environment requires that no non-organization-owned devices are allowed to connect to the organization's internal network, then network logs and audits of those logs may also serve as a monitoring point for the acceptable systems use policy. As with information security controls themselves, monitoring points should be deliberately determined and documented along with the control itself. Results of monitoring activities should also be documented.

**ASSESSING SECURITY CONTROLS**

Assessing information security controls is an ongoing and continuous process as illustrated in Figure 1 in Section III Because the environment in which local governments operate is continually changing, especially in terms of the use of information and supporting technology, security controls must be regularly re-evaluated. Assessment is a key mechanism for the evaluation of controls and may incorporate several components. As information security policies and procedures are documented, a regular interval for review should be determined. A regular, internal policy/procedure review serves to ensure that these documents continue to meet the controls needs of the organization set during the documents' creation, or if changes are required. Internal, regular, full-scale assessments are also important to evaluate the overall control structure against the overall changes to the use needs of and environment in which information is used. Finally, external, full-scale assessments are necessary to have a robust and full-scale information security program. External assessments are designed to provide a broader view of control structures not subject to internal challenges and viewpoints. These components, when well implemented, provide robust protections against unauthorized release of information, malicious use of systems, and other forms of cyber and non-cyber information attacks.

**AUTHORIZING SECURITY CONTROLS**

Like policies and procedures within any of the various functions of government, information security-related policies require authorization at each of the levels at which they apply. In functions such as health care and justice, information security controls are required by regulation. In other cases, such as credit card processing, information security best practices are enforced through stringent application of industry best practices. In all cases, effective information security controls programs are driven by executive leadership. A key role played by organizational leaders in information security is to approve controls. Departmental leaders will likely be involved both in drafting and approving controls for use within their departments. The approval process for departmental controls is often less formal than for approval of organization-wide controls; but, regardless of the level of formality of the approval process, all controls changes should be documented, as noted above.

Organization-wide controls face additional challenges to approval because those charged with approving controls will not always sufficiently understand the controls or the environment in which those controls will be implemented. Lack (perceived or real) of understanding by organizational stakeholders of the concepts that underpin technical controls negatively impacts the security life cycle. If stakeholders don't understand how a control works or why it is necessary, they are not likely to support its implementation or approval. Therefore, it is incumbent on the department head, as the liaison between executive level officials and departmental staff, to ensure that both groups understand and support controls recommendations. In some cases when controls face challenges in the approval process, external resources may be helpful in providing information or new perspectives on controlling risk that may be able to bridge divides among stakeholders. Information technology departmental managers and advocates within the organization face particular challenges to building

understanding of required controls for approval, but should focus on creating controls that meet the needs of approvers, can be effectively implemented, monitored, regularly reviewed, and updated as needed.

**MONITORING SECURITY STATE**

Among the daily challenges of delivering services to citizens, monitoring of internal controls can easily be lost. Keeping track of effective controls can be tedious and the connections among controls monitoring points and the larger mission of the government can seem abstract and distant. Yet, controls monitoring is critical to effective cybersecurity, and more broadly, information security.

Technical controls such as firewalls, switches, authentication systems and workstations have the ability to log activity that can be used to monitor critical functions, which inform the organization's cybersecurity posture and status. By themselves, these devices and logs can be helpful to maintaining information security. But, an effective, organization-wide information security control posture requires integration of various logs and monitoring points so that concerning patterns can be noted and acted upon before an incident occurs. Unfortunately, information technology leaders often find themselves trying to balance between an expensive, integrated, security monitoring solution (manual or technical) and ad-hoc log review that is ineffective at preventing cybersecurity and other attacks on sensitive information. The speed with which the cybersecurity landscape is changing, especially for local governments, prevents any organization from being fully resourced for cybersecurity. Choices must be made. Available resources should be focused on information deemed most critical and sensitive during the information classification step above. When considering the allocation of resources for monitoring of sensitive information, decision makers must take a holistic approach to information and access to it. Information can only be well-secured when the systems and physical locations where it can be accessed are also well-secured. The most effective programs for securing sensitive information integrate cybersecurity controls on systems and technology with broader physical and administrative information security controls. Monitoring security controls, therefore, should focus first on holistic controls coverage for information deemed most critical, and then move to less sensitive information using the same approach.

# VI. HELPFUL LINKS

**Framework for Improving Critical Infrastructure Cybersurity**

National Institute of Standards and Technology (NIST)
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

**State and Local Election Cybersecurity Playbook**

Harvard Kennedy School Belfer Center for Science and International Affairs
https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

**Glossary of Cybersecurity Terminology**

National Initiative for Cybersecurity Careers and Studies
https://niccs.us-cert.gov/about-niccs/glossary

**Indiana Advisory Commission on Intergovernmental Relations Cybersecurity Survey Results**

http://iacir.spea.iupui.edu/documents/CybersecurityBriefIACIR.pdf

**Indiana Cybersecurity Self-Assessment Scorecard Survey**

https://www.in.gov/cybersecurity/files/IECC%20Cybersecurity%20Scorecard%20Public%20fillable.pdf

**Indiana Executive Council on Cybersecurity (IECC)**

https://www.in.gov/cybersecurity/3812.htm

# END NOTES

[1] Taylor, Hugh. (2020, January 22). *What are Cyber Threats and What to do About Them.* The Preyproject.com. https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

[2] Kwiatkowski, Maximilian. (2019, July 17). *County Forced to Pay $132,000 Ransom to Hackers.* Nwitimes.com. https://www.nwitimes.com/news/local/govt-and-politics/county-forced-to-pay-132-000-ransom-to-hackers/article_497cd952-a648-5a72-b280-8254ecd6b229.html

[3] Nolting, Mike. (2017, August 20). *Cyber Attack Reported in Franklin County*. *Wrbiradio.co*m. https://wrbiradio.com/2017/08/20/cyber-attack-reported-in-franklin-county/

[4] Ragan, Steve. (2016, December 8). *After attack, Indiana county will spend $220,000 on Ransomware Recovery*. *Csoonline.com.* https://www.csoonline.com/article/3148274/after-attack-indiana-county-will-spend-220000-on-ransomware-recovery.html

[5] Goudie, Chuck and Christine Tressel. (2018, March 23). *Iranian Cyber Attackers Target State of Indiana and 144 Universities.* Abc7chicgo.com. https://abc7chicago.com/iranian-cyber-attackers-target-state-of-indiana-144-universities/3252887/

[6] Christian, Kurt. (2020, January 3). *Indiana Counties Battle Cyber Attackers with Help from State, Feds, Indianapolis Business Journal.* IBJnews.com. https://www.ibj.com/articles/indiana-counties-battle-cyber-attackers-with-help-from-state-feds

[7] Ibid.

[8] McGalliard, Tad. (2018, March 30). *How Local Governments Can Prevent Cyberattacks*. *Nytimes.com.* https://www.nytimes.com/2018/03/30/opinion/local-government-cyberattack.html

[9] Ibid. Citing the International City/County Management Association and University of Maryland, Baltimore County study.

[10] Christian, Kurt. (2020, January 3). *Indiana Counties Battle Cyber Attackers with Help from State, Feds, Indianapolis Business Journal.* IBJnews.com. https://www.ibj.com/articles/indiana-counties-battle-cyber-attackers-with-help-from-state-feds

[11] National Institute of Standards and Technology Privacy Workshops, https://www.nist.gov/document/nistprivacyriskworkshop6517pptx

[12] McGalliard, Tad. (2018, March 30). *How Local Governments Can Prevent Cyberattacks*. *Nytimes.com.* https://www.nytimes.com/2018/03/30/opinion/local-government-cyberattack.html

[13] Presentation by Mitchell Parker, IU Health.

[14] Ibid.

[15] IT Alliance for Public Sector. *State Cybersecurity Principals and Best Practices*. *Itic.org,* https://www.itic.org/dotAsset/6b96ecc0-53d8-4068-b2a5-4fd79676c9ed.pdf

[16] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology, p. 2. (2018, April 16). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[17] Ibid, p. 7.

[18] Ibid, p. 1.

[19] Ibid.

[20] Ibid, p. 4.

[21] Ibid, p. 14.

[22] Ibid, p. 16.

[23] Ibid, p. 7.

[24] Ibid, 23.

[25] Ibid, p. 7.

[26] Ibid, p. 23

[27] Ibid, p. 6.

[28] Ibid, p. 8.

# NGA Proposal Package

STATE OF INDIANA
OFFICE OF THE GOVERNOR
State House, Second Floor
Indianapolis, Indiana 46204

**Eric J. Holcomb**
*Governor*

March 5, 2021

NGA Policy Academy Review Committee

Re: Application for NGA Policy Academy to Advance Whole-of-State Cybersecurity

Dear Members of the NGA Review Committee:

Cybersecurity is essential to the future stability and economic success of our nation, Hoosiers, and Hoosier businesses.

To effectively protect our residents, businesses, and government entities, Indiana has created a strategic approach built on the support of leaders from government, healthcare, technology, and other critical industries through the framework established by the Indiana Executive Council on Cybersecurity. Since its development, more than 250 leaders from across the state and a broad range of businesses have worked together to suggest and deliver dozens of deliverables, which are free to those businesses and local governments that need them the most.

But there is still much to do, and the support of our fellow states through such efforts as the NGA Policy Academy to Advance Whole-of-State Cybersecurity is vital. By working together, we can establish long-term protection strategies that will provide our residents with the knowledge and infrastructure needed to safeguard against such threats.

Indiana welcomes the opportunity to provide its expertise and join with other states in addressing cybersecurity issues through the Policy Academy. On behalf of our State, we appreciate your consideration in what I am sure will be a successful program.

Sincerely,

Eric J. Holcomb
Governor of Indiana

**State of Indiana NGA Proposal Narrative**
**March 5, 2021**

## Cyber Challenges Facing Indiana

With its unique strategic approach and implementation, Indiana continues to work hard to strengthen the infrastructure of local governments in the Hoosier state. Leadership at the local, state, and federal levels know all too well that local government is among the most vulnerable to cyberattacks, and only in recent years have these municipalities begun taking more critical steps to protect themselves. In a 2020 survey of local government information technology executives by the Public Technology Institute, 54% said their elected officials were only somewhat engaged with cybersecurity efforts, and 23% said their elected officials were not engaged at all. Furthermore, two-thirds of IT executives reported their cybersecurity budget was inadequate. These numbers highlight the importance of focusing on cybersecurity before an event occurs at the local level.

Cyberattacks can, and do, happen in our own backyard. In fact, in recent years local government has experienced firsthand several cyberattacks, including Lawrence County, which was hit by a cyberattack in 2020 that took most of its systems offline for days, and LaPorte County was forced to pay a large ransom after an attack devastated its systems.

## Local Government is Key

Indiana is applying for the NGA Policy Academy to Advance Whole-of-State Cybersecurity's category of Local Engagement and Partnership to develop a *Local Government Cyber Engagement Program.* This program would include a collection of valuable resources and best practices from other industries and states, all in package that is digestible and understandable for a local government unable to afford a cybersecurity staff or state-of-the-art applications. The Program will consist of information, toolkits, templates, guides, training, and resources in a one-stop shop that will address all five areas of NIST's framework: identify, protect, detect, respond, and recover.

## Indiana's Demonstrated Commitment to Cybersecurity

Securing Indiana's information technology infrastructure and industrial control systems is beyond the reach of any single entity; especially as cyber threats became a reality. That is why the Indiana Executive Council on Cybersecurity (Council) was established in 2016 and continued in 2017 through Executive Order 17-11, when Governor Eric J. Holcomb took office, with the renewed focus on how to build and best utilize the cross-sector body of subject-matter experts to effectively understand and prepare for all aspects of Indiana's cyber readiness and resources to stay on the forefront of the cyber risk environment.

As a result, in September 2018 the State of Indiana developed a whole-of-state strategic plan 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. Many of the identified 69 deliverables developed by more than 250 advisory members helped to formulate the detailed 2,000+ page plan, focused on developing resources that can be used by those such as local governments.

Since its development in 2018, the Council and its committees have completed more than 75 percent of the 69 deliverables; a body of work that has saved taxpayers hundreds of thousands of dollars and highlighted Indiana's commitment to bringing Cybersecurity to the Next Level. One key deliverable is the Local Government Working Group's Plan to develop an all-encompassing cybersecurity guide for local government officials and offices. A draft of this deliverable was completed, but it requires the resources and expertise of partners of the IECC and the NGA to develop an effective comprehensive program that can be implemented in a local government as streamlined as possible.

**Anticipated Benefits and Potential Outcomes**
By joining the NGA Policy Academy to Advance Whole-of-State Cybersecurity, Indiana will work with other state leaders to identify successful and proactive ways to work, communicate, and assist local governments in developing an all-encompassing approach to cybersecurity. Using these combined resources, the state believes the help of NGA's comprehensive and actionable *Local Government Cyber Engagement Program* can be developed to the benefit of all Hoosiers.

**Challenges to Implementing Solutions**
Any launch of a successful statewide initiative to local governments in our 92 counties must consider that state and local leadership priorities can change (i.e. pandemic, limited budgets). For the public to recognize and act upon such an important issue, it must be framed and provided in a way that people perceive its importance. The structure of the Council provides for a singular approach to cybersecurity that is consistent in message/scope for all stakeholders.

**Evaluation Plan**
As we work with the NGA, learn from other state best practices, and identify relevant private, state, and federal resources, the team will develop an outline of the *Local Government Cyber Engagement Program.* In that outline, we will identify 3-5 counties and/or local governments throughout the state to test the program, measure the cyber level using the existing Indiana Cybersecurity Scorecard prior to the program as well as after to determine the effectiveness, collect feedback from the pilot group to better the program for the remainder of the counties and provide any key findings to key state leadership and the NGA.

**Team Composition**
The following Core Team Members are Governor appointees on the IECC and like the Home Team Members, they have the resources, connections, and expertise to provide important guidance for the Local Government Cyber Program to be successful.

Core Team: Indiana Cybersecurity Program Director Chetrice Mosley-Romero (Team Lead); Indiana Department of Homeland Security Executive Director and State of Indiana Homeland Security Advisor Stephen Cox; Indiana Chief Information Officer Tracy Barnes; IECC Local Government Chair and Indiana Municipal Management Association Executive Director Rhonda Cook; IECC Local Government Co-Chair and Indiana Association of County Commissioners Executive Director Stephanie Yager; and Indiana Information Sharing and Analysis Center Director Tad Stahl.

Home Team: Office of Governor Holcomb, Office of Lt. Governor, Indiana Office of Community and Rural Affairs, Indiana Department of Homeland Security Communications Director David Hosick, Indiana Chief Information Security Office Hemant Jain, Indiana Office of Technology Communications Director Graig Lubsen, Indiana State Police Capt. Bryan Harper, Indiana State Treasurer Kelly Mitchell, Indiana Broadband Director Scott Rudd, and Indiana Executive Council on Cybersecurity Advisory Members. Administrative Contact: IECC Communications Manager David Ayers

**Supporting Documentation**
The following documentation further shows Indiana has been developing and building upon a successful cybersecurity approach for the last several years, which will all serve as background and purpose for the Local Government Cyber Program:

- Indiana Executive Council on Cybersecurity - Executive Order
- Indiana Executive Council on Cybersecurity - Charter
- Indiana Cybersecurity Strategic Plan – September 2018
- Appendix D.16 Local Government Working Group Final Strategic Plan

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

# NGA PROPOSAL: INDIANA ADDITIONAL DOCUMENTATION

# 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

# Indiana Executive Council on Cybersecurity Council Charter

Last Updated: January 11, 2019

Version: 5

# Table of Contents

## 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.

Additional Voting Members may be appointed at the discretion of the Governor.

## 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) designees 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 and Cybersecurity Program Director.

- 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 designees 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 or her discretion his or her 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
  - Cyber Summit 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

- 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 quarterly, 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.

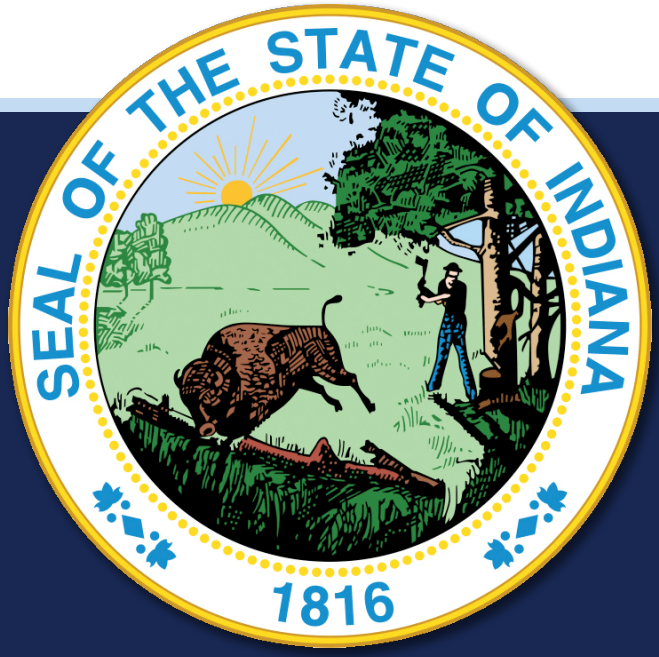
## ARTICLE 6 – NON-EXCLUSION PROVISION

- 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.

# 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,

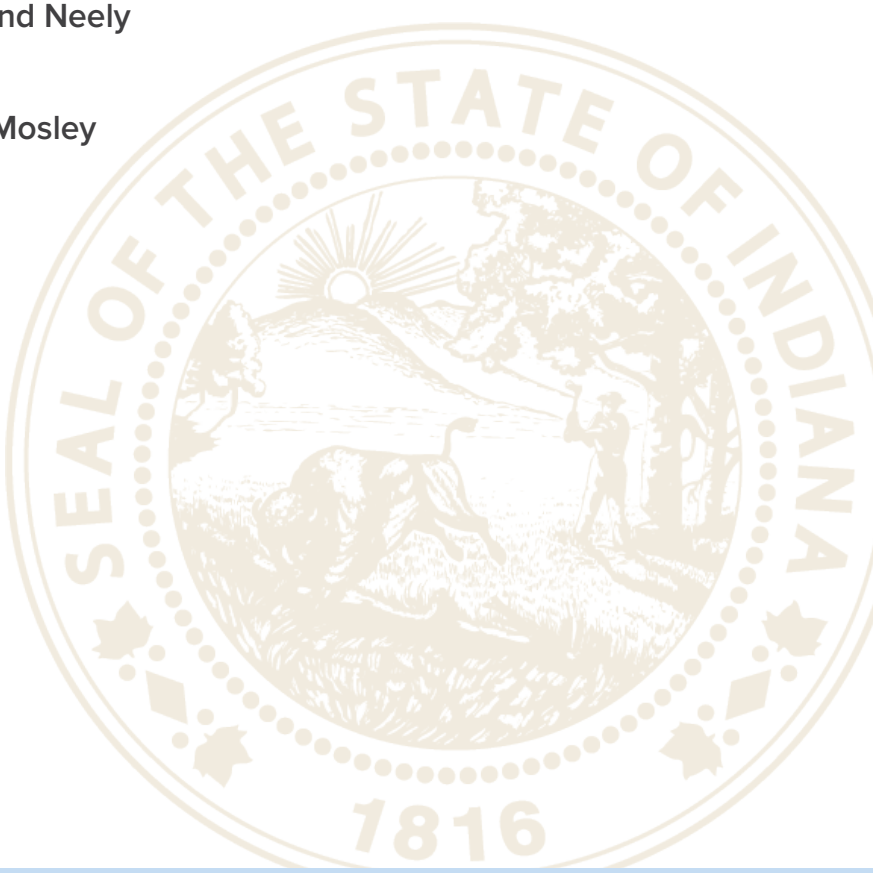
**Executive Director Bryan Langley**
Indiana Department of Homeland Security

**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

# 2018 INDIANA CYBERSECURITY STRATEGIC PLAN

Table of Contents



*...continued on next page*

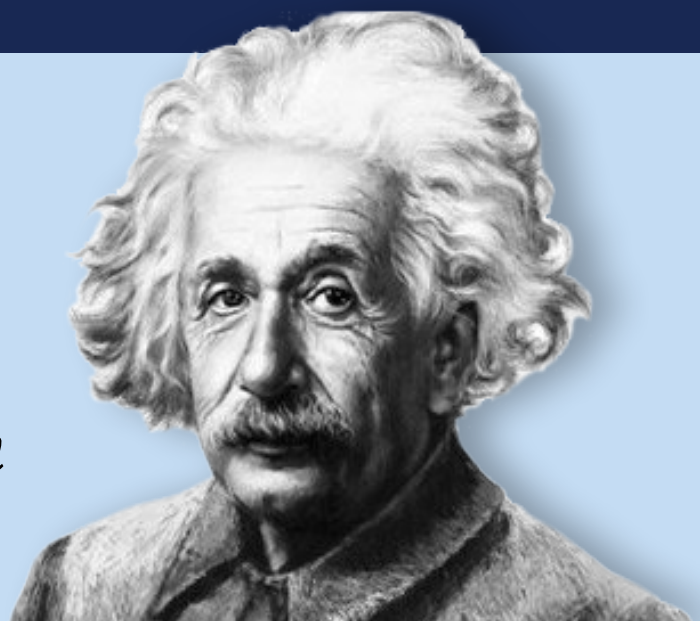
Table of Contents (continued)

## APPENDICES (continued)


# 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.

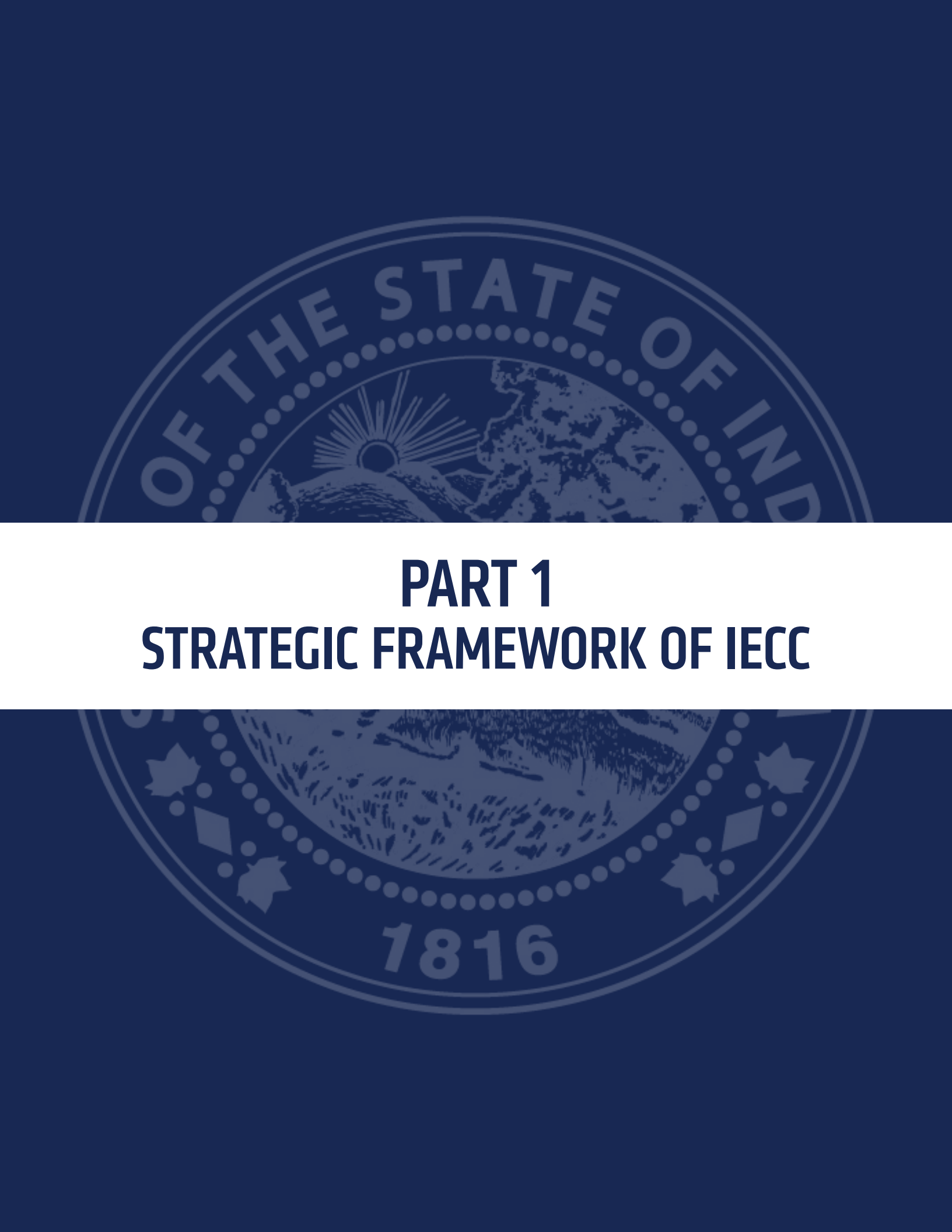
Part One is the Council's strategic framework. It provides the background of the Council, establishes high-level cybersecurity goals, presents the composition of membership, and addresses how it has met the objectives of Indiana Governor Eric J. Holcomb's Executive Order.

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.



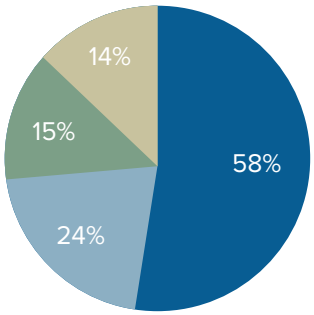
# PART 1
# STRATEGIC FRAMEWORK OF IECC

## 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.

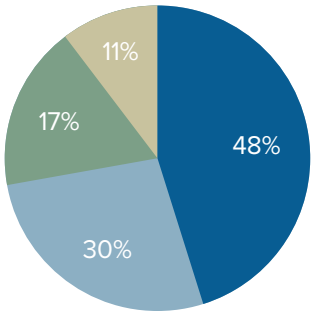
In fact, the 2018 Verizon Data Breach Investigations Report found the victims of breaches to be 58 percent small businesses, 24 percent healthcare organizations, 15 percent accommodation and food services, and 14 percent public sector entities. Of those breaches, 48 percent occurred from hacking, 30 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.

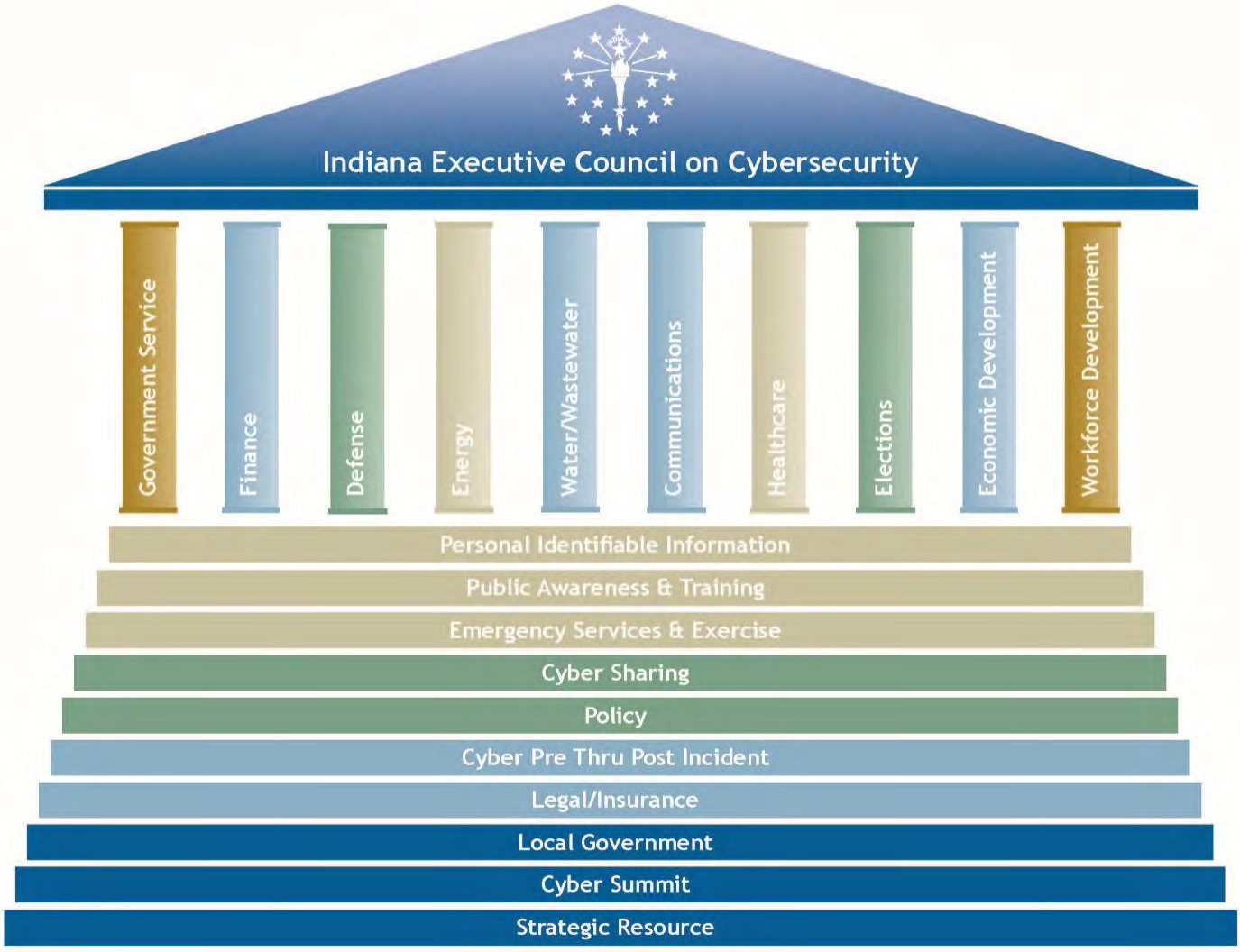



*Figure 1 : IECC Strategic Breakdown*

## 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

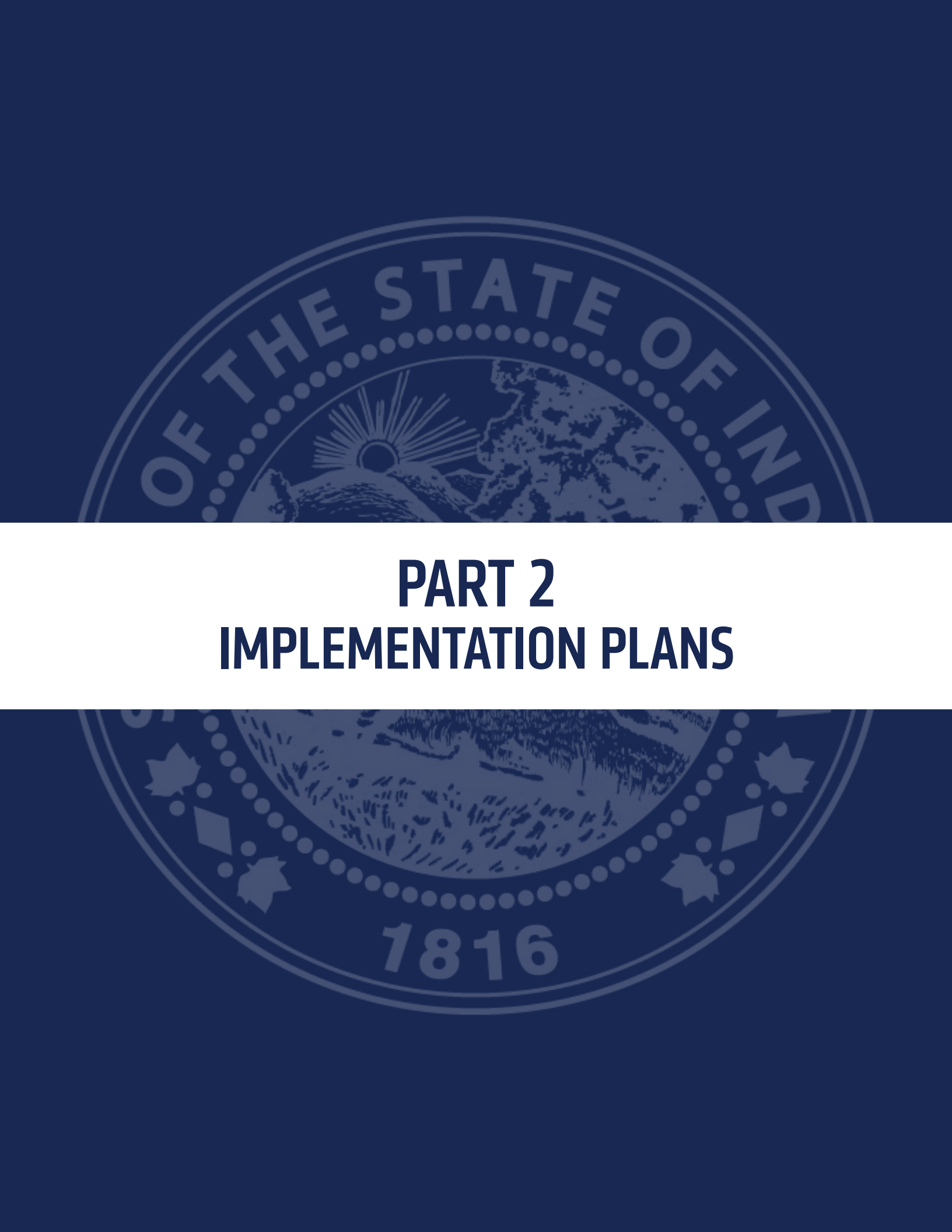
In addition, meetings, facilitated discussions, director oversight, shared online platforms, and tools, were implemented to avoid duplication of developments and deliverables, and to allow for a fully transparent process. This included a consolidated Q&A forum document that was used within and across 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<br>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.

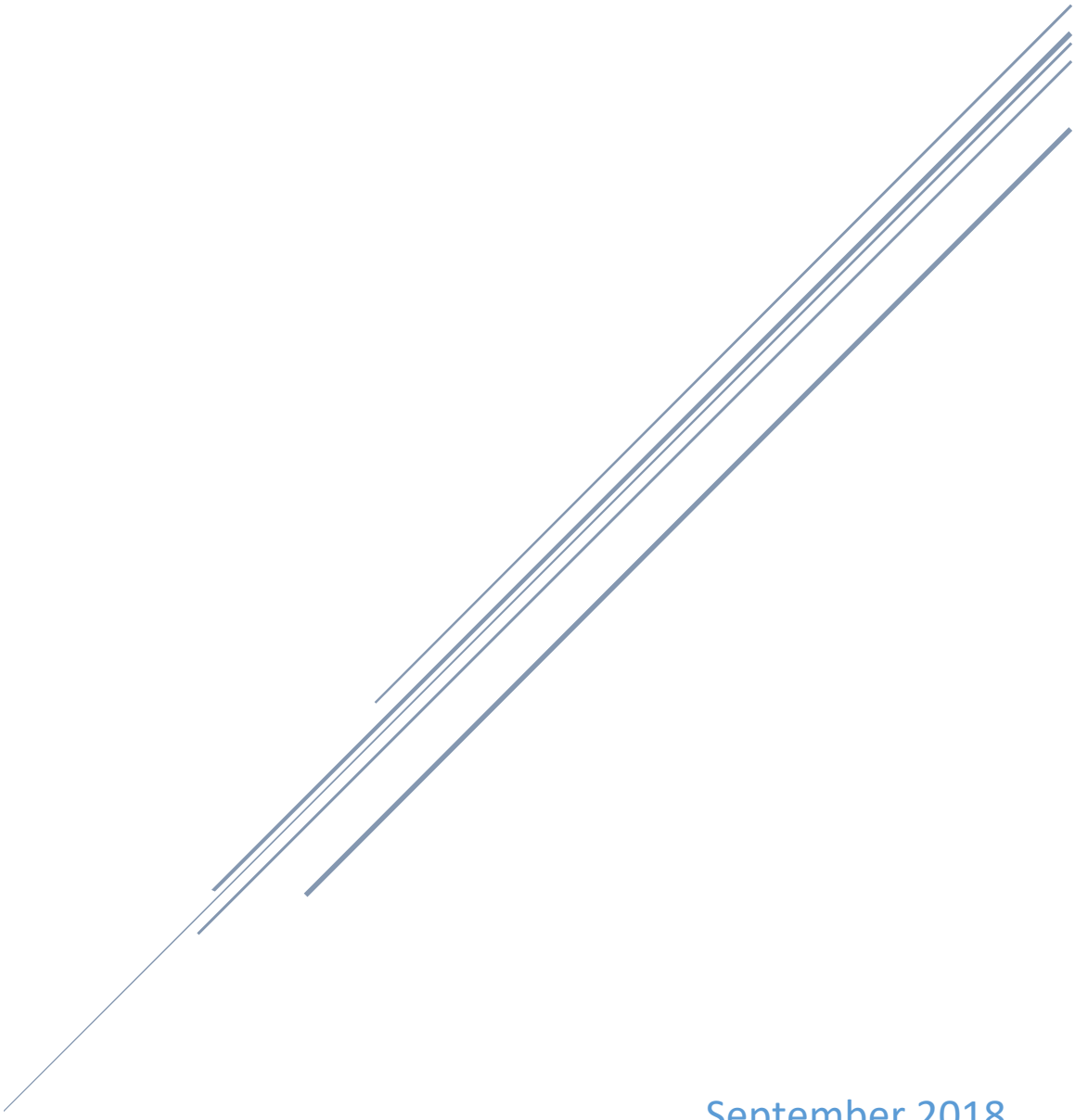
## IECC MOVING FORWARD

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.

# 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

## 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

# Podcast Statistics as of October 2021

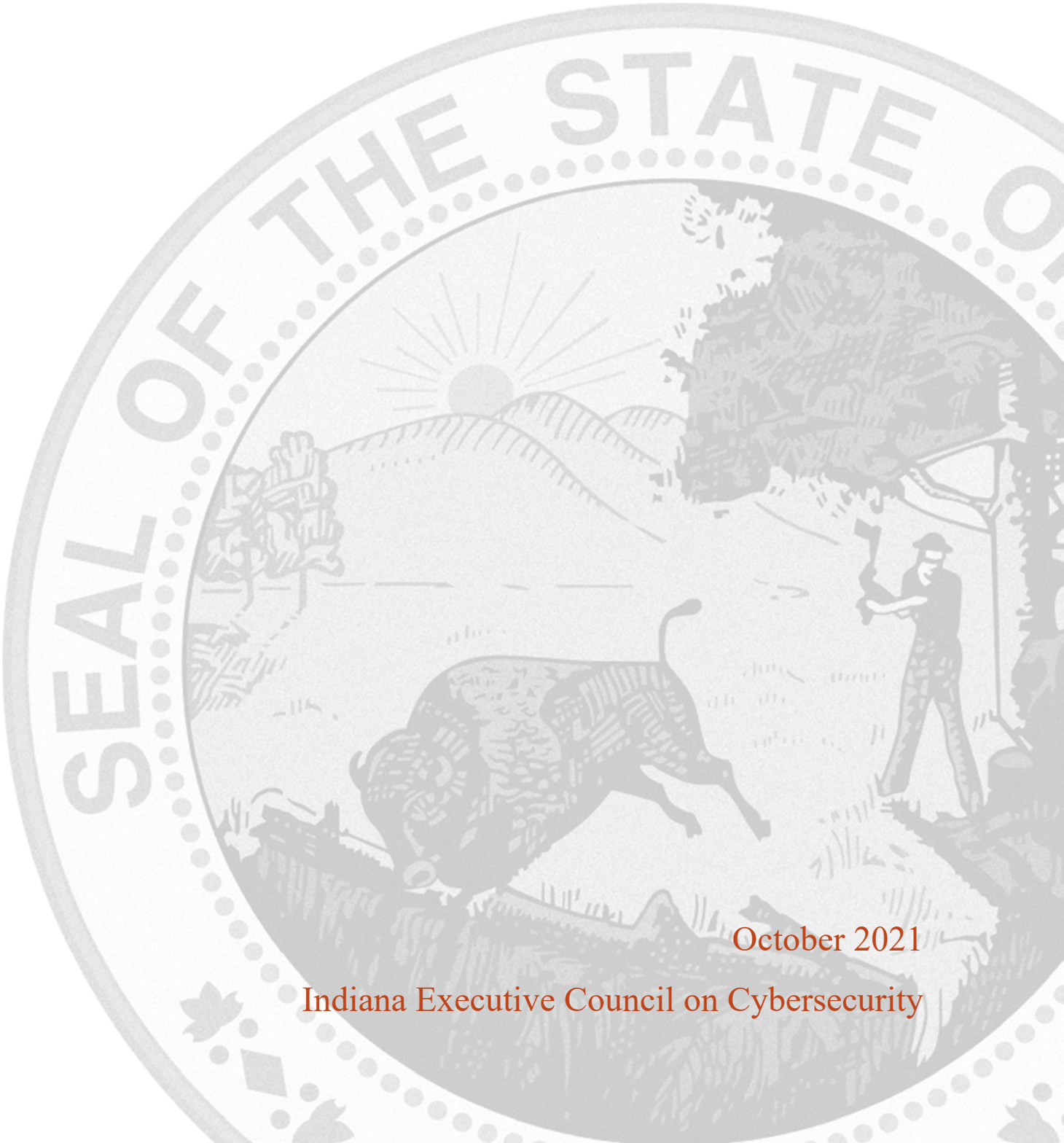
# EXHIBIT A

| # | Release Date | Episode Name | IBB Host? | Treasurer Co-Host? | Chetrice Mosley-Romero Co-Host or Guest? | Guest(s) Name(s) | Guest(s) Affiliation(s) | Total Listens & Views (as of 10/13/21) | Unique Features |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 9/23/2020 | Days of our Cyber Lives Episode 1 | Y | Y | Y | Chetrice Mosley-Romero | IECC (IOT/IDHS) | 119 | First episode; recorded 9/22/20 |
| 2 | 10/6/2020 | Resources for School Communities with IDOE | Y | Y | Y | Dr. John Keller | IDOE | 87 | |
| 3 | 10/23/2020 | Scary Cyber Tales from Local Government (Halloween Theme) | Y | Y | Y | None | N/A | 107 | |
| 4 | 12/19/2020 | Indiana State CIO - Tracy Barnes | Y | Y | N | Tracy Barnes | IOT | 234 | |
| 5 | 2/2/2021 | Hemant Jain - CISO at the State of Indiana | Y | Y | N | Hemant Jain | IOT | 98 | |
| 6 | 2/16/2021 | IU Health Chief Information Security Officer - Mitchell Parker | Y | Y | Y | Mitchell Parker | IU Health | 104 | |
| 7 | 2/22/2021 | Breaking News: Oldsmar Florida Utility Hack | Y | N | Y | John Lucas | Citizens Energy Group | 17 | "Breaking News" podcast |
| 8 | 4/6/2021 | Indiana Department of Revenue - Bob Grennes | Y | Y | Y | Bob Grennes | IDOR | 34 | |
| 9 | 4/12/2021 | National Telecommunications Week | Y | Y | N | Ed Reuter | IN911 | 91 | |
| 10 | 5/17/2021 | National EMS Week (Dep't Homeland Security) | Y | N | Y | Steven Cox | IDHS | 59 | |
| 11 | 5/27/2021 | Breaking News: Colonial Pipeline Ransomware | Y | N | Y | Russ Paluch, Brian Carman | Maverick Energy, IBB | 68 | "Breaking News" podcast |
| 12 | 6/8/2021 | National Association of State Treasurers Live Episode | Y | Y | N | Tracy Barnes, Teri Takai | IOT, Center for Digital Government | 56 | Live, in front of audience, non-Hoosier guest |
| 13 | 6/30/2021 | National Social Media Day - Cybersecurity Tips for Social Media | Y | N | Y | Melissa Thomas, Jennifer Simmons | IEDC, AIM | 61 | |
| 14 | 9/15/2021 | Guest: Tad Stahl (IN-ISAC and 1169) | Y | N | Y | Tad Stahl | IOT | 33 | Last guest episode |
| 15 | 9/28/2021 | Days of Our Cyber Lives Series Finale | Y | Y | Y | None | N/A | 23 | Last episode |
| | | | | | | | **TOTAL** | **1191** | |


# Appendix D.8
## Healthcare Committee

# HEALTHCARE COMMITTEE STRATEGIC PLAN

Chair: Mitchell Parker
Co-Chair: Jacob Butler




October 2021

Indiana Executive Council on Cybersecurity

# Healthcare Committee Plan

# Table of Contents

# Committee Members

# Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Bailey | George | Purdue University / cyberTAP | Assistant Director, cyberTAP / Professional Services | As Needed |
| Berryman | Glenn | Community Health Network | Chief Information Security Officer | Advisory |
| Butler | Jacob | Parkview Health | Manager of Enterprise Systems | Co-Chair |
| Davis | Philip | Community Health Network | Director, IT Risk and Compliance | Full Time |
| Fredland | Valita | Community Health Network | Senior General Counsel | Full Time |
| Hobgood | Lisa | Deaconess Health System | Chief Information Officer | As Needed |
| Johnson | Jason | Parkview Health | IS Manager | Full Time |
| Linder | Jared | Family and Social Services Administration | Chief Information Officer | As Needed |
| Lyle | George | Purdue University | Senior IT Security Risk Analyst | As Needed |
| Mabry | Kevin | Sentree Systems, Corp. | Chief Executive Officer | Full Time |
| Martz | Jeff | Health and Hospital Corporation | Chief Information Security Officer | Full Time |
| Ndow | Emmanuel | Marion General Hospital | Chief Information Officer | As Needed |
| Odum | Matt | Briljent, LLC | President | Full Time |
| Parker | Mitchell | IU Health | Executive Director, Information Systems | Chair |

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Schmidt | Eric | Eskenazi Health | Information Security Officer | Full Time |
| Sturgeon | Nick | IU Health | Director, Information Security | Full Time |
| VanZee | Andrew | Indiana Hospital Association | Vice President of Regulatory and Hospital Operations | Full Time |
| Wichlinski | Robert J. | Great Lakes Labs, LLC | Executive Vice President and General Manager | As Needed |
| Nevers | Frank | Franciscan Alliance, Inc. | Security Program Manager | Full Time |
| Vuppalanchi | Deepika | Syra Health | Chief Executive Officer | Full Time |
| Whitmore | Erica | Anthem, Inc. | Senior Security Risk and Intelligence Analyst | As Needed |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

# 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), andFinancial 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 andDrug Administration (FDA)
    - Jennings Aske, Juris Doctor (JD), CISO, Columbia/New York PresbyterianHealth.
    - Ralph Hall, Leavitt Partners. The committee 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 ofHealth and Human Services (HHS) Office for Civil Rights.
    - Iliana Peters, Acting Deputy Director of Enforcement, HHS Office For CivilRights.
    - Nebraska Hospital Association.
    - Josh Singletary, NH-ISAC.
      - The committee has also utilized several papers and presentations from Mitch Parker and IU Health to provide further research. The papers supplied have 100+ sources each andwere submitted as part of graduate school programs.
      - The committee has continued to research actual attacks and vulnerabilities that have led to attacks. We have examined root causes of numerous ransomware and malware attacks that have led to system downtimes across the world.

- **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 appliesto 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 providerof 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) include 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 ofthe federal government has standardized.
- The H-ISAC is providing all providers with information; however, it is overly technical in nature.
    - While H-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 ruralareas 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 formalInfo 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 Economicand Clinical Health (HITECH) Act, to complete risk assessments of vendors.
- Healthcare organizations are dealing with lower margins, not enough IT staff, and alack of cohesive guidance.
    - The number of vendor risk assessments that medical device manufacturershave to deal with, and the high variety are causing issues with vendors. Jennings Aske is leading an effort to standardize these assessments.
    - While NH-ISAC has the Cyberfit program, which focuses only on applications, licensed by Prevalent, it is also costly at $4,000 per assessment. With the number of vendors and applications that a health system can have, ifused 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. Theseneed to be shared to set global expectations.

- The FDA understands that current medical device security efforts are losing peopleover unclear explanations and not listening to customers.
- According to the FDA, vendors need to be educated on how to present security. Many 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 devicecompanies, is considered incentive enough, indicates Jennings.
- 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 approachrelative 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 based on his six years as a CISO in Minnesota.
- 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. Vincent's, 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.
- According to our research, the dwell time of attacks within healthcare networks is measured in months, and these attackers are taking their time to identify network assets. They are using this information to specifically target backups and other critical information to increase their chances of payment.
- Attacks have occurred locally, including at Eskenazi Health, that have crippled networks at multiple levels.

- **2021 Plan Working Group Deliverables**
  - Long-Term Education
  - Healthcare "Cyber in a Box"
  - Vendor Management Resources
  - Statewide Cybersecurity Exercises
  - Cyber Sharing Platform

- **Additional Notes**
  - None at this time.

- **References**
  - 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. 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 healthsystems 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, 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 havingto keep the lights on in many organizations.

3. **What is your area's greatest cybersecurity need and/or gap?**
   a. The need is 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 (SME) 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. Those in healthcare 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 and Data Security Standards. The organizations who 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. The committee has highlighted the H-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. Included are 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/NYPHealth 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. Others in the medical sector are currently utilizing the same sources Indiana does. There are also self-organizing as part of emergency management to address these issues. This self-organization includes working with H-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?**

   <u>One year:</u>
   - Begin developing a pilot program modeled after H-ISAC's Threat Intelligence Committees (TICs)
   - Collaborate across multiple institutions to address security issues
   - Provide a means for healthcare organizations to contact and to report potential issues.
   - Beginnings of a communication plan designed to reach out to healthcare providers.

   <u>Three years:</u>
   - Expansion of the program to have more dedicated staff and interactionwith providers.
   - More proactive education
   - Collaboration with other states and organizations such as H-ISAC, Infragard, and Department of Homeland Security (DHS) to provide cybersecurity awareness

   <u>Five Years:</u>
   - 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'sand your area's cybersecurity?**
   a. There needs to be a concerted effort to reach out to particular medical providers to specifically address what is needed to increase security. Although the awareness of the need for cybersecurity is high, the specific guidance as to what is needed to be secure has been either too specific or not enough.

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 2020 U.S. Bureau of Labor Statistics, 13 percent 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 35,000 people. Approximately 750 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 hiring to 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 minimum of one.
    f. The issue is not cybersecurity jobs, it is getting people to understand cybersecurityand 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. Facilitating business development and encouraging companies to locate offices and/or staff in Indiana based on the availability of top-level graduates, quality of living, and low cost of living would attract and retain talent.

12. **What are your communication protocols in a cyber emergency?**
    a. Hospital Incident Command System (HICS) is followed to escalate incidents. There is now a 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?**
    a. Focus on assessing risk and helping people understand what to do to address it would be a best practice. There needs to be a focus on the fundamentals of cyber hygiene and privacy measures. Focusing on the cybersecurity as a separate entity independent of overall patient privacy is making it more difficult to attack the root causes of information breaches.

# Deliverable: Long-Term Education

# Deliverable: Long Term Education

## *General Information*

1. **What is the deliverable?**
   a. The deliverable is Indiana-focused versions of security education targeted at small to medium-sized providers. Most of the guidance given out by CMS to providers assumes that providers either have an IT staff or someone with the requisite level of expertise within the organization to interpret guidance and give staff instruction. While working on several other projects, CMS discovered that most small to medium sized providers and critical access hospitals do not have the staff needed to implementsolutions nor have been educated on how to address threats. Most importantly, manydo not know where to report data breaches or cyber-attacks.
   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 organizationsdo 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?**
   ☐ 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.**
   ☐ 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 protectthemselves 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?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Small to medium healthcare entities across the state who do not currently receive thistype 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.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The Health Sector Coordinating Council (HSCC), American Hospital Association (AHA), InfraGard, H-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, H-ISAC, REN-ISAC, Indiana IOT, Indiana Hospital Association,Indiana Health Information Exchange (IHIE), and Health Sector Coordinating Council (HSCC)

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 causemachines to malfunction because of non-functional patches.

## *Implementation Plan*

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

☐ One-time deliverable
☒ Ongoing/sustained effort

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Work with supporting subgroup | JB/Team/Communication Subgroup | 15% | 9/15/2021 | |
| Gather resources | JB/Team | 25% | 10/1/2021 | |
| Define Message Formatting | JB/Team | 0% | 11/1/2021 | |
| Build Delivery Methods | JB/Team | 0% | 2/1/2022 | |
| Implement 2022 LTE/Release | Mitch Parker | 0% | 4/1/2022 | |
| Review Effectiveness of Training, Surveys, and Customer Feedback | Mitch Parker | 0% | 2/1/2023 | |
| Plan 2023 Training | Mitch Parker | 0% | 3/1/2023 | |
| Deliver 2023 LTE | Mitch Parker | 0% | 4/1/2023 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

| 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?**

| Resource | Justification/Need for Resource | Estimated Initial Cost | Estimated Continued Cost, if Applicable | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|---|
| Web Site Space | Space on Indiana Cybersecurity Portal to host data – needed for data sharing and accessibility | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. This will provide Indiana healthcare providers the training materials and information they need to educate themselves about cybersecurity risks, threats, best practices, and strategies.

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

a. This deliverable will educate providers about the cyber risks and what they can do to mitigate those risks /with a minimum of resources. It will provide healthcare providers with information to aid in their understating of security risks and how to leverage strategies to lower their risks.

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

a. Healthcare providers will continue to be not cognizant about how to mitigate their business risks. Small to medium-sized Healthcare providers will not have information they need to continue to grow knowledge of security topics.

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

a. Success is quantitatively defined as the number of providers who download and utilize the education in their practices. The baseline is zero practices using it now. In addition, a customer satisfaction survey is planned to review effectiveness along with feedback. Having ten providers use this would be considered a 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?** ⊤

☒No ☐ Yes

**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?**

☒No ☐ Yes

## Other Implementation Factors

---

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

a. The largest factor is the resources from larger providers and IECC to be able to complete these deliverables effectively given numerous other resource constraints.

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?**

☒No ☐ Yes

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

a. This will need the continual attention of IECC members to plan, develop, and evaluate effectiveness of the deliverables, especially as topics change.

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

a. This committee has decided to leverage resources from CISA, the Health Sector Coordinating Council, and H-ISAC as a base. Continue work with the communication subgroup is needed to ensure consistent communication plans.

**27. Can this deliverable be used by other sectors?**

☒No ☐ Yes

a. The long-term education could be used by all other sectors. However, the data will be constant with healthcare needs.

## Communications

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

a. All healthcare providers and practices in the state of Indiana will need to be informed of its availability using existing notification systems, the state portal, and appropriate communications mechanisms for the website updates.

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

☐No ☒ Yes

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

a. Making several conference presentations about its development and community involvement will be considered.

## *Evaluation Methodology*

**Objective 1:** IECC Healthcare Committee will update Indiana-focused versions of security education in 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

**Objective 2:** IECC Healthcare Committee and partners will provide updated Indiana-focused versions of security education to 80 percent of Indiana healthcare providers in 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

**Objective 3:** IECC Healthcare Committee and partners will collect customer effectiveness, usage, and/or feedback survey for future development in 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

# Deliverable: Healthcare Cyber in a Box

# Deliverable: Healthcare Cyber in a Box

## *General Information*

1. **What is the deliverable?**
   a. Repackaging and organizing the Health Sector Coordinating Council and Healthcare Information Sharing and Advisory Council (H-ISAC) materials for Indiana health care providers to give them a more focused and clear approach to solving health care problems.

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.**
   ☐ 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?** (Chose 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. This will provide templates and base information healthcare providers can use to protect themselves against cyberattacks. This information will also be used to help providers understand their risks and take action to address their gaps.

6. **What metric or measurement will be used to define success?**
   a. The number of providers that utilize this toolkit or parts of it after its creation will define its success.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Small to medium-sized healthcare providers that do not have their own security staff or a security firm available to assist will benefit from this.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. The work from H-ISAC, CISA, and the HSCC overlaps, which is why the focus changed from original content to utilizing much of theirs and repackaging it for healthcare providers.

## 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 coordinating with the Cyber Sharing group, along with multiple other subcommittees to incorporate their materials into the 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?**
    a. The Health Sector Coordinating Council (HSCC), Health ISAC (H-ISAC), CISA, and IECC would all need to be involved.

12. **Who should be main lead of this deliverable?**
    a. Mitch Parker or Jeff Martz.

13. **What are the expected challenges to completing this deliverable?**
    a. Continued healthcare IT resource availability given the number of cyber events that have occurred in the past 18 months.

# *Implementation Plan*

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

☐ One-time deliverable

☒Ongoing/sustained effort

**Tactic Timeline**

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Gather resources | MBP/JM | 25% | 12/31/2021 | Delayed due to Eskenazi cyber event |
| Organize/Select resources | MBP/JM | 0% | 1/1/2022 | |
| Define format for toolkit | MBP/JM | 0% | 2/1/2022 | |
| First draft of toolkit | MBP/JM | 0% | 4/1/2022 | |
| Second Draft | MBP/JM | 0% | 5/1/2022 | |
| Release | MBP/JM | 0% | 6/1/2022 | |
| Communication Plan | MBP/JM | 0% | 6/1/2022 | Info available from IHA, state portal, and through state communications mechanisms about this toolkit |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒ No ☐ Yes

| 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?**

| Resource | Justification/Need for Resource | Estimated Initial Cost | Estimated Continued Cost, if Applicable | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|---|
| Web Hosting | Need to host for providers | $0 | $0 | | | Can use existing IECC web site and Indiana resources |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Provide the small and medium, low-staffed providers with templates to assess and address risks without having to spend significant dollars doing so.

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

a. This deliverable will provide healthcare providers with information they can use to self-assess and understand their risk profile from a good starting point. A basic risk assessment can cost $20,000. This can save providers at least that by giving them the info they need to do one of these on their own.

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

a. Small to Medium-sized Healthcare providers will not have information they need to properly assess and address risks to their environment. This will put them in a position of continuing to put patient data and personal information at risk.

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

a. We define success as the number of providers that successfully download and utilize this toolkit in their own practices to help address risks. The baseline for it is that right now 0 of them are doing so. Even 10 providers using this toolkit significantly improves security and is considered a 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?**

☐No ☒ Yes

**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?**

☐ No ☒ Yes

## Other Implementation Factors

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

a. The prevalence of cyberattacks in the state of Indiana can impact the resources needed to complete this deliverable.

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

☒No ☐ Yes

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

a. This will require IECC Healthcare Committee members to periodically update these documents and the toolkit as regulations and policies change, specifically at the Federal level. They would also need to coordinate to upload them to the Cybersecurity portal.

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

a. The Health Sector Coordinating Council (HSCC).

**27. Can this deliverable be used by other sectors?**

☒No ☐ Yes

## Communications

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

a. We would need to notify healthcare providers across the state of Indiana using existing notification systems, the state portal, and appropriate communications mechanisms for web site updates.

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

☐No ☒ Yes

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

a. We would want to involve IHA and potentially IPLA to notify their constituents of this toolkit.

## *Evaluation Methodology*

**Objective 1:** IECC Healthcare Committee will create a "Healthcare Cyber in a Box" of security education designed for small- to medium-size offices and systems in 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

**Objective 2:** Healthcare Committee and partners will distribute Healthcare Cyber in a Box of security education information to 80 percent of Indiana healthcare providers.

*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 Healthcare Committee and partners will measure feedback/usage of the toolkit by 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

# Deliverable:

# Vendor Management - Healthcare IT Security, Risk & Compliance Handbook

# Deliverable: Healthcare IT Security, Risk & Compliance Handbook

## *General Information*

1. **What is the deliverable?**
   a. A short document resourcing Indiana healthcare practices and organizations of all sizes with needed information to ensure their security programs fit the most up-to-date regulatory requirements, especially with vendors.

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?**
   ☐ 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. To inform Indiana healthcare providers of recent updates in law and to provide accurate resources for practical implementation advice regardless of size.

6. **What metric or measurement will be used to define success?**
   a. An increasing number of Indiana businesses who assess their cybersecurity risks and make informed business decisions based on that review (whether they insure or not).

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Individual Indiana businesses will benefit from making informed cyber risk assessments, suffer fewer compliance penalties, 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 Health Sector Coordinating Council's Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM) overlaps and will be included (https://healthsectorcouncil.org/HIC-SCRiM-v2/).

## 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, Attorney General

12. **Who should be main lead of this deliverable?**
    a. Cybersecurity Council office

13. **What are the expected challenges to completing this deliverable?**
    a. Continued resource allocations given current cybersecurity challenges.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Draft the initial document including key outline of processes and procedures Indiana providers need to implement | IECC Healthcare Committee – Mitch Parker, Philip Davis | 0% | December 2021 | |
| Circulate the document among the IECC Healthcare Committee for revisions and edits | IECC Healthcare Committee | 0% | January 2022 | |
| Implement Committee feedback and finalize document | IECC Healthcare Committee – Mitch Parker, Philip Davis | 0% | March 2022 | |
| Publish final draft on the Indiana Cybersecurity website | IECC Healthcare Committee – Mitch Parker, Philip Davis | 0% | April 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1/8 FTE | 1/8 FTE | Indiana Attorney General staff member skilled in healthcare/HIPAA Security Rule compliance actions | Cybersecurity Council Office | Indiana General Assembly | |

**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 |
|---|---|---|---|---|---|---|
| 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 what Indiana providers need to know regarding their security and risk management programs and practices, state providers will more easily understand federal and state requirements, see fewer fines and compliance penalties, and be able to create more investment in their healthcare services serving Indiana residents.

b. By implementing the security program guidance contained within the document, Indiana healthcare businesses will be more prepared to respond to cyber-attacks and downtimes. As a noted critical infrastructure sector by federal agency Cybersecurity and Infrastructure Security Agency (CISA), Indiana will be contributing to the overall national increased readiness encouraged by the federal government.

**18. How will this deliverable reduce the cybersecurity risk or impact? What are 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.
b. The average cost of a healthcare data breach in 2021 has risen to $9.23 million, up from $7.13 million in 2020 (IBM Security 2021 Cost of a Data Breach Report)
c. The average ransomware attack costs businesses $4.62 million (IBM Security 2021 Cost of a Data Breach Report).

**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 cyber attacks 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. The Cybersecurity Council could set a baseline of Indiana healthcare entities that have had a reportable breach and/or compliance penalties assessed in the year(s) leading up to the guideline publication, and a drop in both areas of breaches and compliance penalties would measure a successful effort.

**21. 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. 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?**

☒No ☐ Yes

a. We are not aware of initiatives in other states.

## 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?**

☒No ☐ Yes

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

a. The ongoing effort will likely be monitoring Indiana healthcare entities who have suffered a reportable healthcare breach and/or received compliance penalties as a result.

**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?**

☒No ☐ Yes

## 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)?**

☐No ☒ 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.

b. The deliverable could be marketed at various healthcare-centric conferences and professional events

## *Evaluation Methodology*

**Objective 1:** IECC Healthcare Committee will draft the initial document including key outline of processes and procedures Indiana providers need to implement by Qtr. 1, 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

**Objective 2:** Circulate the document among the IECC Healthcare Committee for revisions and edits by Qtr. 2, 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

**Objective 3:** Implement Committee feedback and finalize document by Qtr. 2 of 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

**Objective 4:** Publish final draft on the Indiana Cybersecurity website by Qtr. 3 of 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: Exercise

# Deliverable: Exercise

## *General Information*

1. **What is the deliverable?**
   a. The Healthcare Committee will stage two tabletop exercises a year to simulate disasters and cyber-attacks across Indiana. These will be open to IECC members and Indiana healthcare organizations. The first exercise will be run by the IECC, and may include members of the Healthcare ISAC, CISA, Health Sector Coordinating Council, and American Hospital Association. The second exercise will be run with the National Guard at Fort Muscatatuck and will involve real-life simulations using their facility.

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?**
   ☐ 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 goals of these exercises are to:
      - Simulate current cyber-attacks within a safe environment to determine opportunities for improvement
      - Provide information on current capabilities and strengths
      - Give a gap analysis of where to improve and why

6. **What metric or measurement will be used to define success?**
   a. Completion of the exercises
   b. After-action report with areas for improvement

7. **What year will the deliverable be completed?**
   ☒ 2021 ☒ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. The IECC, participating healthcare organizations, recipients of the report, the Indiana National Guard, and other participating organizations would and have benefitted from this.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. The cybersecurity resources from the IECC, IOT, HSCC, and National Guard overlap.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The IECC committee at large on planning, along with the National Guard, CISA, and HSCC to plan an exercise.

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 will need to work with IOT, the National Guard, CISA, and HHS/HSCC to complete this. The AHA and IHA are optional.

12. **Who should be main lead of this deliverable?**
    a. Mitch Parker

13. **What are the expected challenges to completing this deliverable?**
    a. Based upon the 2021 challenges with delivering both tabletops, it comes down to resource and time availability to plan out the scenarios. We also need time at Muscatatuck to effectively plan out the scenarios using their resources and planning.

## *Implementation Plan*

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

☐ One-time deliverable

☒ Ongoing/sustained effort

### Tactic Timeline

**INCyber CISA Exercise – August 11, 2021**

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Prepare with planning partners in initial, mid, and final planning meetings | USDHS CISA and IECC partners | 100 | Jan-July 2021 | |
| Hold Exercise | USDHS CISA and IECC partners | 100 | Aug. 11, 2021 | |
| Review AAR | Cybersecurity Program Director and USDHS CISA | 100 | October 2021 | |

**INNG Homeland Defender Exercise – August 13, 2021**

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Prepare with planning partners in initial, mid, and final planning meetings | INNG and IECC partners | 100 | Aug. 2021 | |
| Initiate cyber IR component | INNG and IECC partners | 100 | Aug. 2021 | |
| AAR | INNG | 50 | TBD | |
| Develop a W/WW workshop to hold virtually | IECC Partners | 100 | October 2021 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|---|
| 0.1 | 0.1 | Planning | | | | |

**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 |
|---|---|---|---|---|---|---|
| Web Conferencing Platform | Needed to host the first tabletop exercise | | | | | |
| Fort Muscatatuck Computing Resources | Needed for real-life simulations of IoT | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. The greatest benefit is the production of quantitative results and action plans that detail opportunities for improvement and areas where organizations can take steps to improve.

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

a. This deliverable reduces the risk and impact of a cyber-attack by providing exact steps and processes organizations can take to reduce them immediately based on the exercise. This can potentially save organizations thousands of dollars, if not more, by allowing them to focus on more immediate threats to their people, processes, and technologies.

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

a. We will not be able to simulate current cyber threats in an environment designed to identify issues for remediation. Organizations within Indiana would not be able to identify and address these threats and dependencies, and not be able to appropriately act if one of these events occurs.

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

a. Success is the completion of the exercise itself. The metrics used to measure success will be the after-action items that are needed to follow up on to address issues discovered during the exercises themselves. The baseline is based on the issues discovered, and the number is proportional to the degree of the 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?**

☒No ☐ Yes

a. Indiana is the only state that we are aware of that has involved federal and non-profit agencies, along with the National Guard, to the degree that we have in these exercises.

**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?**

☒No ☐ Yes

a. There are not currently.

## Other Implementation Factors

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

- Availability of resources at Fort Muscatatuck to help plan and develop the exercises
- Availability of IECC resources to help plan and develop the IECC exercise

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

☒No ☐ Yes

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

a. We will need at least one IECC member and 2 Healthcare Committee members to work on planning these exercises on an annual basis.

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

a. We have been working with Chetrice Mosley, David Ayers, the HSCC, H-ISAC, Indiana National Guard, and American Hospital Association

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes,

a. In 2021 we worked with the Water sector on these. Based on the scenario picked for 2022 we will work with other sectors as identified by the exercise.

## Communications

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

a. The entire IECC community and all Indiana healthcare organizations would be notified to see if they wish to observe or participate.

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

☐No ☒ Yes

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

a. Since this is such a unique event for the state of Indiana, there will be media and conference opportunities to present this. This includes television and print media, along with security conferences such as RSA or Black Hat.

## *Evaluation Methodology*

**Objective 1:** Working with partners, participate in a statewide cyber exercise that affects healthcare industry by August 2021.

*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 partners, participate in an exercise with the National Guard at Muscatatuck by August 2021 that addresses a known cyber vulnerability.

*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 Platform

# Deliverable: Cyber Sharing Platform

## *General Information*

1. **What is the deliverable?**
   a. Cyber Sharing Platform

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

4. **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.

5. **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

6. **What is the resulting action or modified behavior of this deliverable?**
   a. The goal of this cyber sharing platform is to facility sharing of cybersecurity information (i.e., Indicators of Compromise (IOCs), cyber observables, threats, intelligence, tactics, techniques, and procedures) among the healthcare sector at a tactical/technical level. The Healthcare WG will work with the Cyber Awareness and Sharing WG to leverage the IECC Cyber Sharing Community Slack channel to facilitate this deliverable. The resulting action is a grass roots sharing of cyber information in real time.

7. **What metric or measurement will be used to define success?**
   a. Number of IECC members in the IECC Slack Channel.

8. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

9. **Who or what entities will benefit from the deliverable?**
   a. All IECC healthcare members and their organizations

10. **Which state or federal resources or programs overlap with this deliverable?**
    a. DHS HSIN, H-ISAC Threat Intelligence Committee, HSCC

## Additional Questions

11. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Cyber Awareness and Sharing Working Group

12. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable**?
    a. Representation from as many healthcare organizations will be necessary.

13. **Who should be main lead of this deliverable**?
    a. Nick Sturgeon

14. **What are the expected challenges to completing this deliverable**?
    a. Getting involvement from healthcare organizations.

## *Implementation Plan*

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

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Beta Test | Nick Sturgeon | 50% | October 31, 2021 | |
| Go Live | Nick Sturgeon | 0% | November 31, 2021 | |

## Resources and Budget

**16. Will staff be required to complete this deliverable**?

☒No ☐ Yes.

**17. 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 |
|---|---|---|---|---|---|---|
| Slack Channel | This application is the medium in which the sharing will take place. | Free | $8/person | N/A | N/A | To get additional capabilities and features from the slack channel we would need to move up to the Pro plan. Additionally, Salesforce's purchase of Slack may mean additional costs. |

## Benefits and Risks

**18. What is the greatest benefit of this deliverable? What are the estimated costs associated with that risk reduction?**

a. By utilizing the IECC Cyber Sharing Community Slack Channel, it will provide a medium in which the technical cyber security staff of healthcare organizations can share cyber information in real time.

b. This Slack Channel will provide the means of our healthcare organizations and their cyber security/IT staff to share cyber information in real time. This will also allow them to connect with their peers in other organizations at a level they determine is sufficient. This also removes a choke point in sharing information out by elimination the need to rely on one person to share out information. Additionally, individuals can determine what information to share and what information to consume. The biggest cost reduction is time.

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

a. That critical cyber information will not get shared as broadly as needed.

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

a. The definition of success will be the total participation and engagement of the IECC members.

**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. No Response

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

☒No ☐ Yes

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

a. We will need engagement from the IECC member organizations to keep this going.

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

a. IECC Cyber Awareness and Sharing Working Group

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. This deliverable is something that can be used by all sectors.

## Communications

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

a. The healthcare member organizations

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

☒No ☐ Yes

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

a. No Response

## *Evaluation Methodology*

**Objective 1:** IECC Healthcare Committee will Beta Test with the Cyber Awareness and Sharing Working Group by Qtr. 1 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

# 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.

- Vendor Management – Best Practices
- Long-Term Education Materials
- Exercise News Release and Information Sheet

# Vendor Management – Best Practices

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

# Best Practices – Vendor Management

**IECC Partner IU Health has shared the following vendor policies and instructions for other organizations to use as a template for their own.**

**For their entire vendor management program, visit**
**https://iuhealth.org/about-our-system/vendor-relations**

**Indiana University Health, Inc. Standard Information Security Requirements and Demonstration of Compliance for Interfaces**

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. 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, application, or interface 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), 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 is able to securely transmit and receive data in compliance with the HIPAA Security Rule, or HITECH Act, by utilizing Approved hashing and encryption algorithms from the NIST Cryptographic Algorithm Validation Program (CAVP) (https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program). Transport Layer Security (TLS) version 1.2 or greater and 256-bit Advanced Encryption Standard (AES-256) are IU Health's accepted standards for transmission security, and AES-256 is the accepted standard for encryption of data at rest. SHA-2 and SHA-3 are IU Health's accepted standards for cryptographic hashing algorithms.

ii. 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. If stored, login credentials will be hashed and salted using at least SHA-256 or encrypted using at least AES-256 encryption using FIPS 140-2 compliant encryption. At no time will plaintext credentials will be stored unprotected.

    2. For administrative access to the system to make configuration or security changes, two-factor authentication utilizing a secure application or physical token generating a cryptographically-generated key, or federation to a platform that performs it will be required.

    3. For services running on Microsoft Windows, utilization of Group Managed Service Accounts to run Windows Services will be required when possible.

    4. Authentication utilizing OAuth2 for customer-facing and authenticated Application Programming Interfaces (APIs) is required.

    5. User authentication needs to utilize OAuth2, SAML v2, Azure Active Directory, or similar federation technologies whenever possible.

iii. 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.
3. 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.).
4. Demonstrated reviews of firewall and Web Application Firewall (WAF) configurations to validate and verify minimum necessary rules are in place and that misconfigurations which can allow unauthorized access are avoided.
5. Demonstrated security scanning of the environment that includes credentialed and non-credentialed vulnerability scans of the internal and external environments, with a specific focus on addressing Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) issues.
6. Demonstrated security scanning and vulnerability remediation of Application Programming Interfaces (APIs) that includes credentialed and non-credentialed vulnerability scans internally and externally, and full testing of APIs to the Open Web Application Security Project (OWASP) API Security Top 10 Security Project and OWASP Top 10 vulnerability types.
    a. Usage of Web Application Firewalls, API Gateways, or similar mitigation mechanisms to address vulnerabilities will not be considered valid vulnerability remediations by IU Health.
7. Static code analysis utilizing a verified third-party tool to ensure provided source code does not have any known security issues.
8. Security mechanisms on Source Code Control systems to track commits, pulls, or check-ins for potential security issues including trojan horses, malicious code, or backdoors inserted into source code using software supply chain toolsets such as in-toto (https://github.com/in-toto).
9. Digital signing of code and executables developed for the IU Health environment utilizing at least SHA-2 hashing algorithms and checksums.
10. Continual security monitoring of developer workstations, build environments, test machines, servers, and source code control systems.
11. Endpoint Detection and Response (EDR) software on developer workstations, build environments, test machines, source code control systems, and other systems used in the product development environment.
12. Periodic vulnerability testing of the environment to discover and remediate potential vulnerabilities.
13. If the product or service sends email on behalf of IU Health to team members or customers, the systems used to send email on behalf of IU Health must comply with Domain-based Message Authentication, Reporting, and Conformance (DMARC), DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF). This is to protect against fraudulent emails being sent to recipients.

iv. Provide support for the application(s) or interface(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)

v. If there are discovered security vulnerabilities in the previously described items and/or the application(s)/interface(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.

vi. If there are discovered security vulnerabilities in the previously described items and/or the application(s)/interface(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.

vii. 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.

Indiana University Health

## Information Security

# Indiana University Health, Inc. Guidelines on International Data Usage

The purpose of this exhibit is to set the requirements and guidelines by which IU Health data can be accessed by foreign third parties outside the United States and Canada. Due to the increased risk of data exfiltration and low enforceability of agreements across borders, IU Health has put these requirements and guidelines into place to protect stakeholders.

i. Data Hosting Location. IU Health data must be hosted in the United States, Canada, or a mutually agreeable location where data will be protected under appropriate privacy laws. IU Health will approve the ultimate destination(s) of data.
   a. If data is stored in a mutually agreeable location, the appropriate supervisory authorities will be contacted and advised. Appropriate documentation, such as a Data Protection Impact Analysis and supporting documentation under the European Union General Data Protection Regulation (GDPR) will be filed with them and shared with IU Health.
   b. Whenever possible, data stored outside the United States will be verified and validated using distributed technologies and cryptographic hashing used to keep copies of the hashes in multiple locations, including locations within the United States, even if the data itself resides outside the US.
      i. Distributed systems used to store these hashes must meet IU Health security requirements, detailed in the Indiana University Health Verification and Validation using Distributed Computing Requirements appendix.

ii. Data Access. Access to data outside the United States, Canada, or the agreed-upon location will be via remote or virtual desktop technology using two-factor authentication based upon strong cryptography using technology agreed upon by the vendor and IU Health.
   a. Text message-based authentication is not allowed due to interception risk.
   b. Devices used to access data must meet or exceed IU Health Security Standards

iii. Data Processing. IU Health data must be processed and/or have analytics performed on it in the United States, and the results of the analytics must be stored there.

iv. Data Security. Data stored outside the United States must be stored in facilities that are ISO 27001 certified.

v. Cloud Security. Data stored outside the United States with Cloud providers must be stored with ISO 27017/27018 certified providers. The provider must be certified for the region(s) the data will be stored in.

vi. Restricted Countries and Entities. IU Health forbids Business Associate or any of its subcontractors or subservice providers from directly employing resources or contracting for services on its behalf from countries on the US Department of the Treasury Office of Foreign Asset (OFAC) Control Sanctions Programs list, available at https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx. IU Health also forbids Business Associate or any of its subcontractors or subservice providers from directly employing resources or contracting for services on its behalf from people or companies on the US Commerce Department Bureau of Industry and Security Consolidated Screening List, available at: https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern

## Information Security

# Medical Device Security and Responsible Vulnerability Disclosure

1. **Medical Device Security Standards**
    a. Medical Devices in the scope of this agreement that are required to meet IU Health Security Standards include devices that have:
        i. Serial (RS-232, RS-485, etc.), Ethernet, Wireless Ethernet, Bluetooth, ZigBee, Cellular data, or other technologies that allow the wired or wireless transmission of data or signals over radio frequencies to another device or computer.
        ii. Persistent storage on the device itself such as a hard drive, solid state disk (SSD), or flash memory.
        iii. Universal Serial Bus (USB) ports.
        iv. Secure Digital (SD) or other forms of removable storage.
        v. A Central Processing Unit (CPU) and Random Access Memory (RAM) used for performing its essential functions.
        vi. A computing device attached to assist the device in performing its intended function.
    b. Applicable devices need to meet the requirements stipulated in the IU Health Standard Information Security Requirements and Demonstration of Compliance exhibit.
    c. Additionally, applicable devices need to demonstrate compliance with either the FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices guidance, and/or the Underwriters Laboratories (UL) Standards for Software Cybersecurity for Network-Connectable Products (UL 2900-1).
2. **Responsible Vulnerability Disclosure Policy**
    a. Vendor hereby agrees to permit Indiana University Health (“IU Health”) and its subcontractors to conduct product and application security testing of devices in the scope of this agreement without limitation or restrictions and with the intent to identify potential security vulnerabilities in the software, hardware, devices, antennae, related configurations, and other properties available (“potential vulnerabilities”) on the devices in scope of this agreement.
    b. IU Health agrees equipment upon which any security testing is performed will not be placed in patient care operations. IU Health agrees to disclose potential vulnerabilities to Vendor at no unreasonable day and within 90 days of IU Health identification.
    c. Vendor agrees to provide a vulnerability mitigation plan to IU Health within 7 days of report and make product enhancements available within 90 days should IU Health, according to its own definition, determine the vulnerability prevents safe device utilization.
    d. Furthermore, Vendor agrees to publicly disclose potential vulnerabilities as soon as reasonably possible and at least within 90 days of receipt from IU Health.
3. **Medical Device Security Incident Costs**
    a. In the event of a Security Incident which Covered Entity or other entity with Privacy and Security Rules enforcement jurisdiction determines was proximately caused by nonconformance with the terms and conditions described in Indiana University Health, Inc. Standard Information Security Requirements and Demonstration of Compliance, Business Associate shall be responsible for all costs associated with the incident, including but not limited to: (i) Updating of device firmware and software to mitigate the vulnerability which caused the Security Incident to a current, non-vulnerable version; (ii) Updating of software on associated computing devices, servers, and supporting technology infrastructures to current, non-vulnerable versions; (iii) Remuneration for time spent by internal or contracted IU Health resources to mitigate the vulnerability; (iv) Reconfiguration of the Medical Device environment to conform to the Terms and Conditions in the Security Exhibit; (v) Retesting of the environment by IU Health Information Security or a third party to verify and validate that the Medical Device environment conforms to the requirements of the Standard Information Security Requirements and Demonstration of Compliance exhibit.

Indiana University Health

## Information Security

# Indiana University Health, Inc. Payment Card Industry – Data Security Standards Requirements

These are minimum requirements required by IU Health's Information Security Program for technologies used on behalf of IU Health for processing payment, credit, or debit cards in accordance with the Payment Card Industry – Data Security Standards (PCI-DSS) set by the PCI Security Standards Council. These are minimum acceptable security standards for protecting this information.

Any information technology system implemented as part of this Agreement that processes, stores, transmits, or receives payment, credit, or debit card information is subject to these requirements. Therefore, any system implemented as part of this agreement must:

i. Demonstrate full compliance with the PCI-DSS standards and associated amendments, available at https://www.pcisecuritystandards.org/ by demonstrating how IU Health will be able to achieve a successful Attestation of Compliance (AOC) by a Qualified Security Assessor (QSA) with the proposed solution.
ii. Work with IU Health to maintain full compliance, verifiable with successful Attestations of Compliance (AOC) with PCI-DSS security standards throughout the product lifecycle by developing an operational management plan to ensure currency of all in-scope components, including operating systems, supporting software, and third-party libraries.
iii. When the PCI-DSS standards update to a new version, provide an operational plan to ensure IU Health's compliance with it before the retirement date of the previous standard.
iv. If any part of the PCI-DSS solution is outsourced, provide the following for review by both the Enterprise Architecture and Information Security teams on an annual basis or upon update of the systems in scope to the current standards version:
    a. A PCI-DSS Attestation of Compliance (AOC) for the current standards version completed by a certified Qualified Security Assessor (QSA). We will not accept self-attestations or any substitute documentation.
        i. We will accept a verified successfully completed AOC in lieu of an IT Risk Assessment (ITRA).
    b. A Service Organizations Control Level 2 (SOC 2) report and HITRUST Common Security Framework (CSF) certification letter or ISO 27001/27018 certification by a certified accountancy for remote or cloud-based hosting facilities.
    c. A data flow diagram showing payment card data flow from entry to ultimate disposition of data.
    d. A network architecture implementation diagram demonstrating required segmentation, firewall rules, and network protection including firewalls, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), Data Loss Prevention/Cloud Access Security Broker technologies (DLP/CASB), Security Incident and Event Management Event Logging (SIEM), and strong cryptography.
    e. Demonstrated reviews of firewall and Web Application Firewall (WAF) configurations to validate and verify minimum necessary rules are in place and that misconfigurations which can allow unauthorized access are avoided.
    f. Demonstrated security scanning of the environment that includes credentialed and non-credentialed vulnerability scans of the internal and external environments, with a specific focus on addressing Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) issues.
    g. Ensure that third parties that provide scripts or services to support the credit card processing environment have sufficient security controls, including PCI-DSS Attestation of Compliance where appropriate, to prevent malicious hijacking of their scripts. This is to help prevent Magecart-type attacks where credit card data is sent not only to its legitimate destination, but also to malicious third parties.
    h. Storage of Restricted or Critical data behind a stateful network firewall, ideally logically segmented and not stored on a device with a directly Internet-accessible Internet Protocol (IP) or Internet Protocol v6 (IPv6) address.
    i. Demonstrated two-factor authentication for administrative system access utilizing system(s) compliant with the NIST Special Publication 800-63B standards.
    j. Demonstrated provisioning and identity validation/proofing processes that are compliant with NIST Special Publication 800-63B standards.
    k. If the Business Associate or Third Party will not be compliant with the above, a documented explanation must be provided in a timely manner along with associated risk mitigation strategies.

v. If the PCI-DSS solution involves the collection of credit, debit, or payment card data over phone or voice telecommunication services, the standards in the PCI Standards Security Council Information Supplement, Protecting Telephone-Based Payment Card Data, must be followed for the most current version of the document available.
    a. The solution must be validated and certified by a certified QSA before production operations.
vi. Ensure that all in-scope devices promptly remediate discovered vulnerabilities in the operating system, applications, cryptographic subsystems, and third-party support software within seven (7) days.
vii. Enforce, utilizing network-based and logical controls, that only authorized parties can read, write, or otherwise access PCI-DSS data.
viii. Actively block traffic from malicious sources identified by the Financial Services Information Sharing and Advisory Center (FS-ISAC) and its member institutions.
ix. Enforce, utilizing network-based, logical, and physical controls, that the assets participating in the scope for PCI-DSS are only allowed to connect to systems or services required for authentication, disaster recovery, minimum necessary data interchange, administration, or maintenance.
x. Enforce, utilizing a combination of network-based and contractual controls, the following security controls and practices to address network-based spoofing and interception attacks, including BGP Hijacking and DNS Hijacking:
    a. Participant(s) will make sure that the internetworking infrastructure hosting distributed computing services in the scope of this agreement have Autonomous Service Numbers (ASNs) registered with the American Registry for Internet Numbers (ARIN – www.arin.net) or the equivalent for their geographic area(s).
    b. Participant(s) will make sure that all networking prefixes advertised by the ASNs for routing are properly registered with ARIN or its equivalent(s).
    c. Participant(s) will make sure that all networking providers that exchange traffic through peering arrangements filter announcements of their registered and advertised network address space by non-registered ASNs.
    d. Participant(s) will make sure that the provider(s) providing the internetworking infrastructure hosting their services have staffed Network Operations Center(s) operating 24 hours a day, 7 days a week.
    e. Participant(s) will make sure that the following service level agreements are in place with their provider(s):
        i. 5 minute alerting on network failures or issues with Border Gateway Protocol (BGP) or Domain Name Services (DNS).
        ii. 30 minute escalation to an on call network engineer who can make changes to Border Gateway Protocol (BGP) policies or DNS configurations in real time.
xi. Allow IU Health to audit information systems in the scope of the system(s) in scope of this agreement, including mutually agreed-upon penetration tests and vulnerability scans by the IU Health Information Security team or a certified Qualified Security Assessor.
xii. Allow IU Health to monitor the health of and system connectivity of information systems in the scope of the system(s) in scope of this agreement.
xiii. Allow IU Health to monitor the security posture of information systems in the scope of the system(s) in scope of this agreement, including operating system vulnerabilities, application vulnerabilities, network vulnerabilities, and cryptographic system vulnerabilities.
xiv. Provide strong, mutually agreeable, documented, and auditable processes for provisioning, validating, and verifying the identities of all parties with access to PCI-DSS data in accordance with NIST Special Publication 800-63B standards.
xv. Destroy all data no longer in use or required to be retained using a National Association for Information Destruction (NAID – www.naidonline.org) certified provider for PCI-DSS data.

# Indiana University Health, Inc. Smart Contract Security Requirements

These are minimum requirements required by IU Health's Information Security Program for technologies used on behalf of IU Health to provide intelligent contracts, colloquially known as Smart Contracts, on behalf of IU Health. We recognize that this is a technology that can provide significant benefits to IU Health through their use to provide both contracts and automated responses to changes. The purposes of these requirements are to ensure that the underlying technologies utilized on behalf of IU Health are properly assessed and monitored for vulnerabilities that may compromise their integrity, that the contracts work as intended and designed, that IU Health has verification and validation that they are able to work in their intended environment, and that IU Health has reasonable and appropriate controls and measures to prevent intentional or unintentional misuse. 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.

i. Each Smart Contract needs to have a defined written use case, preferably in Unified Modeling Language (UML) format or a similar format that defines:
    a. Sender(s)
    b. Recipient(s)
    c. Input(s)
    d. Output(s)
    e. Actor(s)
        i. Blockchain/Distributed Ledger Technology (DLT) system that it will execute on
        ii. Other Contract(s)
        iii. Oracles, which are external resources that can trigger contract execution
        iv. Interfacing systems and methods
        v. Externally accessible media or files.
    f. Execution Conditions
    g. Preconditions
    h. Postconditions
    i. Programming Language Used
ii. All Smart Contracts need to be validated by a third-party Smart Contracts Validation Service which performs security and integrity testing on contracts to ensure that the contracts perform as intended. Of note, EY is specifically excluded due to their conducting financial services audits for IU Health.
    a. Contracts need to be tested by a neutral third party that does not have an interest in the contract or its outcomes or performs audit services for IU Health.
    b. Contracts need to be tested in a separate environment from the production environment.
        i. Both Business Associate and IU Health will provide non-production systems to the third-party validator to test use cases.
    c. As part of the validation testing, contracts need to be tested for the following:
        i. Race Conditions. This is when multiple concurrently executing contracts achieve different results based on timing and execution, and execution becomes dependent upon the timing, not the instructions within of the contract.
        ii. Reentrancy Attacks. This is when a smart contract can be interrupted in the middle of its execution and instructions to be used for the purpose of exploiting code vulnerabilities to transfer assets or resources outside the bounds of the contract to another party.
        iii. Concurrency Testing. Contracts need to be tested to ensure that multiple simultaneous running copies do not cause race conditions, reentrancy attacks, or behavior outside intended conditions.

iv. Timestamp Dependencies. Contracts need to be tested to ensure they are not dependent upon timestamps for conditions of execution, as this can potentially cause a Race Condition, Reentrancy Attack, or Concurrency issue leading to execution outside of defined bounds and exploitable vulnerabilities.
v. Resource Usage. Contracts will be tested to ensure that they execute instructions consistently and use a defined range of resources.
vi. Access to external resources and Oracles must be tested as part of the validation process.
vii. Upstream and downstream data interchange that occurs as part of the contract must be validated.
viii. Contracts must use validated Application Program Interfaces (APIs) and methods to communicate with upstream and downstream systems.

d. Media or files associated with Smart Contracts need to be stored on globally accessible media using InterPlanetary File System (IPFS).
    i. Pinning, which is the permanent storage of resources on IPFS, needs to be enabled for the lifetime of the contract for all associated media or files.
    ii. DNSLink, which uses Domain Name Services to map a domain name to an IPFS resources, needs to be configured and enabled for resources utilized in Smart Contracts.
    iii. When the hashing algorithm used on IPFS is changed, which changes the resource name, the DNSLink name must be updated.
    iv. Sensitive files must be encrypted using the public key(s) of the recipient(s).
e. Audit logging of all activities must occur, preferably using a Blockchain-based system to ensure their integrity.
    i. The audit log system utilized must meet the requirements in the Indiana University Health Verification and Validation using Distributed Computing Requirements appendix.
f. Zero-knowledge proofs must be utilized for Smart Contracts that contain sensitive or regulated information.
g. Blockchain systems and networks that host and execute these contracts must follow the security requirements in the Indiana University Health Verification and Validation using Distributed Computing Requirements appendix.

Indiana University Health

## Information Security

# Third Party Information Security Practices Due Diligence

### Service Organization Control Reports, HITRUST Common Security Framework (CSF) certification, or Annual Risk Assessments.

Due to the increased security, availability, processing integrity, confidentiality, and privacy risks of using Business Associate and associated subservice providers to deliver Services to or on behalf of Covered Entity, Business Associate agrees to provide to CE an attestation of its and its applicable subservice providers that handle IU Health Confidential Information security risk assessments via an IT Risk Assessment (ITRA), ISO 27001/27017/27018 certifications, or Data Protection Impact Analyses and associated documentation, and Service Organizations Control Level 2 (SOC2) reports every year. A Health Information Trust (HITRUST) Common Security Framework (CSF) certification to the current framework will be accepted for every other year. 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.

i. *Health Information Trust (HITRUST) Common Security Framework (CSF) Certification.* If Vendor has provided proof of HITRUST certification, allow IU Health the right to review their HITRUST assessment certification letter in lieu of an IT Risk Assessment and SOC2 report.
    a. The HITRUST certification must be kept current within 1 year of review and be conducted by a certified assessor.
    b. The version of the CSF attested to must be current within 1 year of review.
    c. Vendor must provide a copy of the certification letter to IU Health, which has the name of the assessor and the version of the HITRUST Common Security Framework (CSF) that has been attested to and certified.
    d. If the certification lapses or is not to a reasonable current framework version as described in (2), IU Health will immediately require a SOC 2 report and full IT Risk Assessment (ITRA).

ii. *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, "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.

iii. *ISO 27001/27017/27018 Certification.* If Vendor has provided proof of ISO 27001/27017/27018 certification, allow IU Health the right to review their ISO certification in lieu of an IT Risk Assessment and SOC2 report.
    a. The ISO certification must be kept current within 1 year of review and be conducted by an accredited certification body (e.g. ANSI-ASQ National Accreditation Board [ANAB]) or a certified accountancy.
    b. Vendor must provide a copy of the certification letter to IU Health, which has the name of the assessor and the ISO standards that have been attested to and certified.
    c. If the certification lapses or is not to a reasonable current framework version as described in (2), IU Health will immediately require a SOC 2 report and full IT Risk Assessment (ITRA).

# Information Security

iv. *European Union General Data Protection Regulation (GDPR) or similar governmental level privacy regulations.* If Vendor has provided proof of compliance with the below, IU Health will review in lieu of an IT Risk Assessment and SOC2 Report. The deliverables need to be in the form of:
    a. A completed Data Protection Impact Assessment (DPIA) or equivalent, including risk assessment and risk management plan.
    b. An assigned Data Protection Officer who has oversight and responsibility for execution of the DPIA, and the review and remediation processes.
    c. Evidence of communication with supervisory authorities about the DPIA, risk assessment, and risk management plan.

v. *Manufacturer Disclosure Statement for Medical Device Security (MDS2) – 2019 revision.* If vendor has provided a completed MDS2 statement for their medical device (not supporting hardware or software), and the MDS2 form submitted is using the 2019 revision of it or later, IU Health will accept this in lieu of an IT Risk Assessment. Older versions do not address current and emerging risks.

vi. *Information Technology Risk Assessment (ITRA).* If the Business Associate cannot provide evidence of HITRUST or ISO certification, sufficient evidence of compliance with GDPR or similar applicable regulations, or a valid MDS2 2019 form for their medical device, the Business Associate needs to Provide IU Health responses to the provided Vendor Risk Assessment and Security Questionnaire.

Any misrepresentation on any of these documents may result in contract termination.

# Indiana University Health, Inc. Verification and Validation Using Distributed Computing Requirements

These are minimum requirements required by IU Health's Information Security Program for technologies used on behalf of IU Health to provide verification and validation services utilizing distributed computing. Such technologies include Blockchain, which is its current and most common usage. We recognize that this is a technology that can provide significant benefits to IU Health through their use to validate and verify transactions. The purpose of these requirements is to ensure that the underlying distributed computing technologies utilized on behalf of IU Health are properly assessed and monitored for vulnerabilities that may compromise their integrity, and the data and systems they are meant to provide integrity for. 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 that utilizes distributed computing technologies to provide verification and validation services to ensure the integrity of IU Health data is subject to these requirements. Therefore, any system implemented as part of this agreement must:

i. Demonstrate that no data that can be classified as Protected Health Information (PHI), Payment Card Industry-Data Security Standards (PCI-DSS), Family Educational Rights and Privacy Act (FERPA), or Privacy Act data will be stored as part of these systems.
ii. Demonstrate that only minimum necessary data from source systems is used to generate cryptographic hashes using a SHA-256 or greater hashing algorithm which will be stored on said Distributed Computing Service.
iii. Demonstrate that no single entity will have control of more than 50% of the total computing power available to process transactions for distributed computing services. This is because if one entity has control of more than 50% of the computing power, they will be able to alter transactions and compromise system integrity.
iv. Ensure that all participants in the distributed computing service promptly remediate discovered vulnerabilities in the operating system, applications, cryptographic subsystems, and third-party support software that directly interfaces with it or produces data to be utilized by the service within seven (7) days.
v. Ensure that all participants in the distributed computing service have a security management program in place to cover not only the assets involved in the distributed computing service, but also all other assets in the purview of the organization.
vi. Enforce, utilizing network-based and logical controls, that only authorized parties can read, write, or otherwise access the Distributed Computing services.
vii. Enforce, utilizing network-based, logical, and physical controls, that the assets participating in the distributed computing service are only allowed to connect to systems or services required for authentication, disaster recovery, minimum necessary data interchange, administration, or maintenance.
viii. Enforce, utilizing a combination of network-based and contractual controls, the following security controls and practices to address network-based spoofing and interception attacks, including BGP Hijacking and DNS Hijacking:
    a. Participant(s) will make sure that the internetworking infrastructure hosting distributed computing services in the scope of this agreement have Autonomous Service Numbers (ASNs) registered with the American Registry for Internet Numbers (ARIN – www.arin.net) or the equivalent for their geographic area(s).
    b. Participant(s) will make sure that all networking prefixes advertised by the ASNs for routing are properly registered with ARIN or its equivalent(s).
    c. Participant(s) will make sure that all networking providers that exchange traffic through peering arrangements filter announcements of their registered and advertised network address space by non-registered ASNs.
    d. Participant(s) will make sure that the provider(s) providing the internetworking infrastructure hosting their services have staffed Network Operations Center(s) operating 24 hours a day, 7 days a week.
    e. Participant(s) will make sure that the following service level agreements are in place with their provider(s):

   i. 5 minute alerting on network failures or issues with Border Gateway Protocol (BGP) or Domain Name Services (DNS).
   ii. 30 minute escalation to an on call network engineer who can make changes to Border Gateway Protocol (BGP) policies or DNS configurations in real time.

ix. Allow IU Health and other members of the Distributed Computing services to audit information systems in the scope of the system(s) in scope of this agreement.
x. Allow IU Health and other members/users of the Distributed Computing services to monitor the health of and system connectivity of information systems in the scope of the system(s) in scope of this agreement.
xi. Allow IU Health and other members/users of the Distributed Computing services to monitor the security posture of information systems in the scope of the system(s) in scope of this agreement, including operating system vulnerabilities, application vulnerabilities, network vulnerabilities, and cryptographic system vulnerabilities.
xii. Allow IU Health and other members/users of the Distributed Computing services to terminate all access to any information systems which have not been patched or remediated for vulnerabilities within seven (7) days as they pose a risk to the integrity of the system.
xiii. Provide strong, mutually agreeable, documented, and auditable processes for validating and verifying the identities of all participants in the Distributed Computing system.
xiv. Provide verifiable Public Key Infrastructure digital certificates and identities to identify all participants that are issued by a mutually agreeable third party. Self-signed certificates are not acceptable.
xv. Ensure that all data elements utilized as part of the distributed verification and validation system undergo data quality checks. This is to make sure that we only utilize verified and validated data as inputs.
xvi. Ensure that transactions recorded as part of the distributed verification and validation system can be reconciled against transactions from the source computing resources.
xvii. Ensure that identities used to publish transactions to the distributed verification and validation system can be verified, and the cryptographic identities of the series of transactions said identities made can be validated.
xviii. Demonstrate third-party risk management processes by mapping cryptographically verified identities involved in transactions to legal entities, and identifying and reconciling all legal entities in the transaction chain.
xix. Ensure that there is a documented method and process for appending records to the system to amend existing records in case of a correction.
xx. Ensure that there is a governance process by which disputed transactions can be arbitrated and amendments posted to the distributed verification and validation system.

Indiana University Health

## Information Security

# Indiana University Health, Inc. Wireless, Cellular, Real Time Location System (RTLS), Radio Frequency Identification (RFID), and Near Field Communications (NFC) Requirements

These are minimum requirements required by IU Health's Information Security Program for technologies used on behalf of IU Health for the implementation or usage of Real Time Location Systems (RTLS), Radio Frequency Identifier (RFID), or Near Field Communication (NFC) systems. As these technologies have the potential to be used to support patient tracking, supply chain operations, patient engagement, and tracking of equipment and assets, IU Health needs to ensure that the data and algorithms used by these systems is demonstrably accurate and protected.

Any information technology system implemented as part of this Agreement that implements these technologies is subject to these requirements. Therefore, any system implemented as part of this agreement must:

i. Define exactly what use cases the solution(s) will be utilized for in the IU Health environment.
ii. Ensure that this system will not store Protected Health Information (PHI), Personally Identifiable Information (PII), Payment Card Industry-Data Security Standards (PCI-DSS), or Family Educational Rights and Privacy Act (FERPA) data.
    a. Payment Solutions that utilize Near Field Communications, such as Apple Pay, are covered by the PCI-DSS security requirements and are exempt from these requirements.
iii. Only utilize minimum necessary data to achieve the desired use cases.
iv. Use system-generated numbers or identifiers that are not based on PHI, PII, PCI-DSS, or FERPA data.
v. Utilize mapping and location information supplied by Design & Construction and Telecommunications.
vi. Ensure that there is adequate wireless coverage for the areas and defined use cases for successful operation of the solution.
vii. Ensure that there is no interference with existing wireless solutions.
viii. Whenever possible, provide enclosures or mechanisms to reduce the potential for signal interception.
ix. Follow cabling and installation standards as defined by the IU Health Telecommunications team in their standards documentation.
x. Systems must be able to be segmented from the main corporate network and communicate over a defined set of network addresses, ports, and protocols to a defined set of IP addresses.
xi. Systems used to send and receive collected data and transmit/receive said data to and from official systems of record, including Enterprise Resource Planning (ERP), Electronic Medical Record (EMR) systems, or other designated IU Health applications, must run vendor-supported operating systems, databases, and supporting libraries, and be patched against known vulnerabilities.
xii. If the solution contains Bluetooth 4.0 or greater or Bluetooth Low Energy (LE):
    a. Security Levels 2, 3, or 4 must be enabled using at least 128-bit Advanced Encryption Standard (AES-128) and Elliptic Curve Diffie-Hellman Key Exchange (ECDHE).
    b. Bluetooth LE Privacy Mode must be enabled to prevent eavesdropping of individual Media Access Control (MAC) addresses.
xiii. If the solution utilizes Near Field Communications (NFC):
    a. Change the encryption keys from the default settings.
    b. Follow the security standards in the ECMA-385 standard, NFC-SEC-NFCIP-1 Security Services and Protocol.
xiv. If the solution supports Wireless Internet utilizing Wi-Fi:
    a. Support the latest standards that IU Health supports.
    b. Support WPA2 or WPA3 authentication to encrypt data in transit and protect against improper alteration of data.
xv. If the solution supports cellular technologies, either Long Term Evolution (LTE/4G) or IMT-2020 (5G):
    a. Solution must be deployed using 5G network slicing to isolate application traffic to a defined segment if using direct device connectivity whenever possible.

b. If the solution utilizes site to site connectivity, Software Defined Wide Area Networking (SD-WAN) technologies must be used to protect communications.
c. All transit utilizing LTE or 5G networks must be actively monitored for security events.
d. Demonstrated reviews of firewall and Web Application Firewall (WAF) configurations to validate and verify minimum necessary rules are in place and that misconfigurations which can allow unauthorized access are avoided.
e. Demonstrated security scanning of the environment that includes credentialed and non-credentialed vulnerability scans of the internal and external environments, with a specific focus on addressing Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) issues.
f. Periodic vulnerability testing of the environment to discover and remediate potential vulnerabilities.
g. All equipment utilized in the transit of data from the access points to the termination point at the IU Health network must be kept current and protected against security vulnerabilities.
    i. Any equipment utilized in the transit of data must not be from a prohibited vendor covered under Section 889 of the National Defense Authorization Act (NDAA) of 2019.
h. Enforce, utilizing a combination of network-based and contractual controls, the following security controls and practices to address network-based spoofing and interception attacks, including BGP Hijacking and DNS Hijacking:
    i. Participant(s) will make sure that the internetworking infrastructure hosting distributed computing services in the scope of this agreement have Autonomous Service Numbers (ASNs) registered with the American Registry for Internet Numbers (ARIN – www.arin.net) or the equivalent for their geographic area(s).
    ii. Participant(s) will make sure that all networking prefixes advertised by the ASNs for routing are properly registered with ARIN or its equivalent(s).
    iii. Participant(s) will make sure that all networking providers that exchange traffic through peering arrangements filter announcements of their registered and advertised network address space by non-registered ASNs.
    iv. Participant(s) will make sure that the provider(s) providing the internetworking infrastructure hosting their services have staffed Network Operations Center(s) operating 24 hours a day, 7 days a week.
    v. Participant(s) will make sure that the following service level agreements are in place with their provider(s):
        1. 5 minute alerting on network failures or issues with Border Gateway Protocol (BGP) or Domain Name Services (DNS).
        2. 30 minute escalation to an on call network engineer who can make changes to Border Gateway Protocol (BGP) policies or DNS configurations in real time.

xvi. Provide a monitoring system, model processes, and support in detecting the following fraudulent usage scenarios:
    a. Unauthorized tag or device cloning.
    b. Multiple instances of tag or device IDs.
    c. Unauthorized alteration of stored values on devices or tags.

xvii. Provide structured asset management data on all devices or tags that can be imported into an enterprise asset management system, including but not exclusive to:
    a. Serial Number
    b. Device Name
    c. Device Type
    d. Media Access Control (MAC) Addresses
    e. Firmware Version.
    f. Date of Manufacture.
    g. Warranty Dates.

# Long-Term Education Materials

# How to develop and execute a patch management routine (CMMC L1)

Mitchell Parker, IU Health


Indiana University Health

## Why are we here?

- Any software application including operating systems, firmware, or plugin installed on a system could provide the means for an attack
- Many software vendors provide patches and updates to their supported products in order to correct security concerns and to improve functionality
- This session will ensure that you know how to update and patch software on each device you own

## What is the requirement/control?

- From NIST 800-171/CMMC L1  3.4.2e
- Employ automated mechanisms to detect the presence of misconfigured or unauthorized system components and remove the components or place the components in a quarantine or remediation network that allows for patching, re-configuration, or other mitigations.

## Why is it important?

- This helps us protect against known vulnerabilities
- It also is item #1 in any DOD Security Technical Implementation Guide
  - Right before configuring least privilege
- You can't have least privilege if you can get around it easily
- It also is a massive issue if you don't patch

## How Does it Protect My Information?

- According to Tripwire [1]: 27% of data breaches caused by unpatched vulnerabilities
- Patching security vulnerabilities measurably protects information from known issues that can be used to exfiltrate data

- [1] https://www.tripwire.com/state-of-security/vulnerability-management/unpatched-vulnerabilities-breaches/#:~:text=Unpatched%20Vulnerabilities%20Caused%20Breaches%20in%2027%25%20of%20Orgs%2C%20Finds%20Study,-Ray%20Lapena&text=In%20May%202019%2C%20Verizon%20Enterprise,Breach%20Investigations%20Report%20(DBIR).

## What are the consequences of not implementing this control?

- Data Breaches
- Security Issues
- Reputational Harm
- Regulatory Issues/Fines
- Loss of Credibility
- Lack of Ability to Keep Environment Current

## OK, what do I really need to do?

- Assume that I don't know IS management well however understand how to run a business – not going to assume you are clueless or inferior

## Inventory

- Get an inventory of all the devices in your environment
  - Including Network Devices!

- Also get an inventory of what software you have both on premises and the cloud
- You want to refer to the 7/30/2020 presentation on Methods to inventory and document organizational hardware and software from TCC Solutions – available at: https://mep.purdue.edu/news-folder/20-cyber-topics-in-20-weeks-series-schedule-free/
  - This goes into much greater detail!

## Assign someone to keep track

- Assign someone to keep track of them – they do not have to be technical – just keep it updated – manage like a business!
  - Name
  - Description
  - Vendor
  - Contract term
  - Responsible user
  - Sw version
  - Purchase date
  - Number of copies
  - End of support date

## What are free or low-cost options to implement the control?

- Make sure you are running a supported operating system
  - If you're running Raspbian, Ubuntu, or Debian, open up a terminal window and type:
    - Sudo apt update;sudo apt upgrade
  - If you're running Red Hat or CentOS, open up a terminal window and type:
    - yum update –security

## Include all devices

- Include HVAC, embedded systems, and your facilities management systems
- Too often we ignore these and have critical business functions running on obsolete hardware and software

## Determine Support Dates

- Determine software dates for software packages and libraries:
  - Check Vendor Web Sites for software separately bought and installed
  - If it comes with Windows, MacOS, or Linux, will be updated by the OS update programs
  - For the OSes themselves, we've provided instructions for the most popular ones:

## Devices Covered

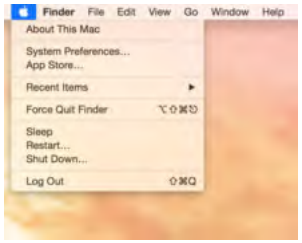
- How do we know if a device is supported?
- Linux:
  - Ubuntu: https://wiki.ubuntu.com/Releases
  - Red Hat: https://access.redhat.com/support/policy/updates/errata
  - Debian: https://wiki.debian.org/DebianReleases
  - Raspberry Pi: https://www.raspberrypi.org/downloads/
- MacOS:
  - https://support.apple.com/en-us/HT201222
- iOS/iPadOS:
  - Only the current version gets updates

## Devices Covered

- Android:  Generally only within the past year
- Windows:
  - https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet
- Chromebooks:
  - https://support.google.com/chrome/a/answer/6220366?hl=en

# MacOS

- Click Here:




- Click About This Mac
- Click Software Update:

# MacOS

- You will then get this screen.  Click Update Now to update

## iOS/iPad OS

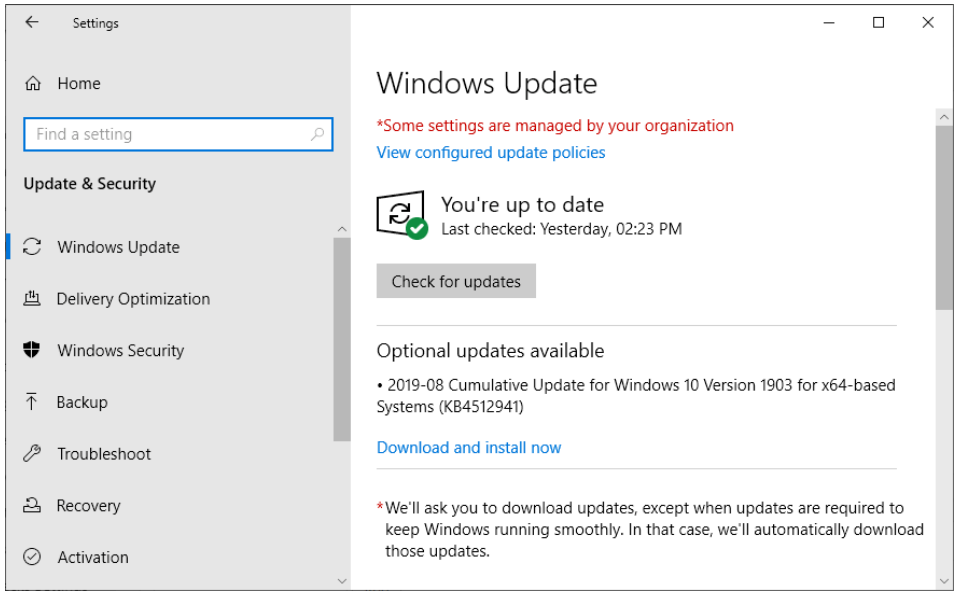
- Go to Settings From the Home Screen:

# iOS/iPad OS

- Go to General -> Software Update -> Download and Install

# Windows

- Go to Settings -> Windows Update and click on Check for Updates:



## Android

- Since this is complex, we just point to the instructions here:
- https://www.lifewire.com/check-updates-for-android-1616953

## Chromebook

- Google provides a link to instructions in one place
- https://support.google.com/chromebook/answer/177889?hl=en
- If your device is supported, this should work

## What else do I need to patch?

- Operating Systems
- Applications
- Database Systems and Services
- Supporting Libraries

## Additional Caveat

- If you have a Zebra industrial device, you will need to contact them to get software updates under a software support contract!

## Planning to Update

- If something is 1-2 years out for not receiving patches, plan to replace it
- If you have a smartphone, plan for 2 years for a Samsung, 3-4 for an Apple, and everything else replace within a year
  - Because patches don't come for older Android devices
- If you have older devices, build plans to update/upgrade them

## How do I do that?

- Build a monthly schedule to:
  - Check for patches
  - Communicate with customers and let them know what's going on
  - Test patches
  - Apply Them in Production

## What do I do if I can't patch something?

- How do I isolate it with wired network equipment?
  - Create a separate Virtual Local Area Network (VLAN)
  - Use your firewall to only allow communications to/from this network to only ports and protocols your application explicitly needs
  - Only allow administrators access to ports needed for remote administration and systems management
  - This may slow performance however is the best alternative for wired equipment

## What if I can't patch something?

- How do I isolate it with a Raspberry Pi or older PCs?
  - Configure a firewall on the device using IPFire (www.ipfire.org)
  - Only allow incoming ports for what's absolutely needed
  - Configure Secure Shell or VPN to access ports for what else is needed

## What if I can't patch something?

- How do I isolate older WiFi?
  - Get a secondary wireless access point or SSID broadcasting on a different channel
  - What are the effects on WiFi I need to consider?
    - Slower speed for all devices
    - Less security for newer devices
    - If you don't manage, less security for all devices
  - They can't take advantage of newer security and lower the security to the lowest common denominator – so keep them isolated!

## What if I can't patch something?

- There's effects on data interchange
- Less secure newer systems
- Less secure data interchange – potential for interception and alteration of data
- We need to keep systems patched and updated so we can secure data interchanges
- That old FTP doesn't "just work". It can be intercepted and your data can be taken!

## Let's recap…

- Inventory
- Assign someone to keep track and manage it like a business
- Include All Devices
- Keep track of support dates
- Patch OSes, Applications, Databases, and Supporting Devices
- Plan to Update
- Have a plan for when you can't patch to isolate
  - Especially Wireless!

## Thank you!

- Thank you for your time!
- Email: mparker17@iuhealth.org
- Twitter: @mitchparkerciso

# Proactive and Preventative Vendor Security Management

Mitchell Parker, Executive Director, Information Security, Indiana University Health


Indiana University Health

# Agenda

- Statement of Issue
- Background on Security
- Mergers and Acquisitions
- Background on Devices and Systems
- Business Drivers
- What has happened?
- Where do we start?
- The five key areas of technology management
- Conclusion

## Learning Objectives

- Recognize the requirements for implementing an effective vendor management program for technology
- Apply knowledge learned from this presentation to proactively improve vendor relations
- Analyze existing vendor agreements and outsourcing contracts and be able to modify them to support information security initiatives
- Develop effective requirements and goals for Clinical Engineering to accomplish either via statements of work or program management to support security requirements
- Define and measure the effectiveness of an enterprise-wide preventive security program and demonstrate metrics to senior management

## Statement of Issue

- We have too much vendor technologies and not enough guidance on how to effectively manage security for them
- In the past decade, as we've increased the usage of Electronic Medical Records, and have automated manual processes, we've connected a significant number of new technologies to the network
- There has not been a corresponding increase in expertise with cybersecurity on many fronts

## Background on Security

- Medical Providers are not all large academic healthcare institutions
  - According to the American Medical Association, in 2014, 60.7% of the medical providers out there are small practices with 10 or fewer physicians.
    - Source: https://www.ama-assn.org/press-center/press-releases/ama-study-finds-majority-physicians-still-work-small-practices
  - According to the American Hospital Association in 2016, the average operating margin was 6.7%, with 30.6% of hospitals having negative operating margins
    - Source: https://www.aha.org/system/files/2018-05/2018-chartbook-table-4-1.pdf

## Background on Security

- Medical Providers are not all large academic healthcare institutions
  - According to the Nebraska Hospital Association in a personal interview, 75% of the hospitals in their state are rural and in small towns
    - These hospitals don't have IT departments. They have outside consultants or someone doing IT as a side job
    - Rural and Critical Access Hospitals, as a rule, have people that have multiple skills or jobs

## Background On Security

- Many of these providers and hospitals do not have the staff to maintain security
- They are lucky if they have staff to maintain the EMR
- We are at an inflection point with new technologies where the security world is going to get turned upside down on providers again
  - New WiFi standards (WiFi 6, 802.11ay)
  - 5G/Reliance on Cellular Service
  - Sunsetting of legacy technologies such as Pagers
  - Shift to Consumerism

## Mergers and Acquisitions

- There has been significant acquisition activity with health services companies actively making deals changing the system landscape
  - Pennsylvania alone has had UPMC, Jefferson, Penn Medicine, and Tower Health reshape the landscape since 2014
  - New Jersey has had Hackensack Meridian and Barnabas Health do the same
  - Advocate/Aurora in the Midwest has also had impact
  - CHS has had both significant acquisitions and divestures nationally
  - According to PwC's US Health Services Deals Insights Q3 2018, there were 261 transactions in Q3 2018, and over 200 in each quarter since Q4 2014
    - Source: https://www.pwc.com/us/en/health-industries/publications/pdf/pwc-us-health-services-deals-insights-q3-2018.pdf

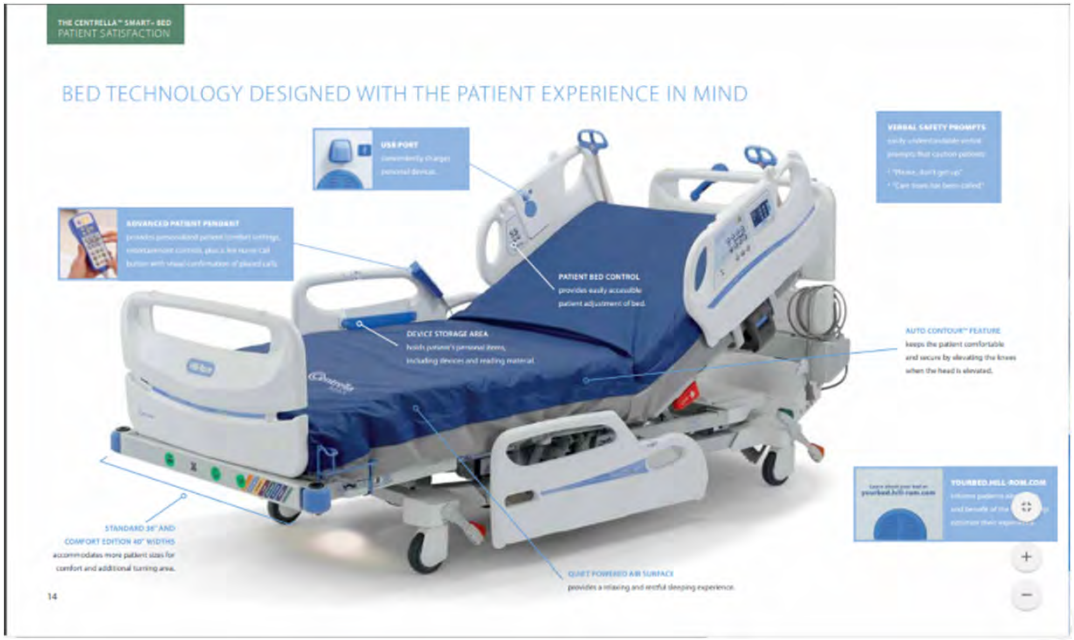
## Background on Devices and Systems

### 1. How does this all relate to them?

- We have had to get very smart about cybersecurity as part of the "M&A Playbook" very quickly for both
- Medical devices, which at one time were considered a capital expense like a bed or supplies, are computer systems in themselves
  - Scratch that part about the bed…the new ones are full-fledged systems in themselves!
  - Not having a plan as you acquire/divest will lead to risks later

# Background on Devices and Systems

- Smart Bed Example:



# Background on Devices and Systems

## 2. More about devices…

- They are pervasive
- They are now part of the care process
- They originally were never meant to be networked in a TCP/IP network
  - Serial devices, yes, where a continual data stream could be sent uninterrupted
  - Ethernet and TCP/IP are very different than Serial
  - Wireless is even more difficult to account for (no lines)
  - 5G/Cell-based technologies have to take more into account
  - PACS/DICOM is an exception to this
- This change is still a major challenge that vendors are working on as it greatly increases complexity!

## Background on Devices and Systems

### 3. Appliances

- These were mainly designed as appliances that require basic upkeep
- We've managed them the way we always have, which is by either:
  - A small Clinical Engineering Team
  - Outsourced Third-Party Contractors
  - Consultants
  - The Vendors themselves

# Background on Devices and Systems

## 4. Networking

- We've put them on the same networks as other devices
  - This is not out of ignorance – people willing to accept risk
  - Not everyone understands networking or security well
  - Not everyone has resources to have a full security program
  - This exposes devices that were never meant to be put on large networks with lots of traffic to exactly that
    - Manufacturers are still grappling with the change from serial to TCP/IP
    - Upcoming FDA guidance speaks of encryption and key management
    - We are increasing complexity significantly!

# Background on Devices and Systems

## 5. Smaller Offices = Consumer/Small Office Devices

- Connectivity to a lot of smaller offices is done using consumer equipment
  - Think Linksys, Belkin, Netgear, or what the local store carries
  - Consumer equipment doesn't have the long support lifecycles of gear from Palo Alto, Cisco, or Fortinet
  - It also is a lot easier to set up for non-IT professionals
  - When you have limited resources, you're not going to put something in that has a high chance of breaking and can't quickly fix or replace. You're going to go to Wal-Mart or someplace within a 30 minute drive
    - When you need something quickly and have patients waiting, you are not going to wait

# Background on Devices and Systems

## 6. Vendor Support

- This is also done for vendor support purposes. It's easier for a tech to remote into a PC and then connect to a device or system either over USB or the network if it's on the same segment than to put in a persistent VPN connection
  - VPN connections open up additional risk
  - We can't expect medical offices that run on consumer grade equipment to even know what IPSec is
  - It's hard for software developers to grasp the nuances of networking and PKI
    - Numerous breaches caused by insecure security implementations prove that
      - **Heartbleed and variants**

## Background on Devices and Systems

### 7. Aftermarket Devices

- We have a very large aftermarket of used devices across the world
  - Smaller facilities and those in non-First World countries buy these devices used
    - They are not always cleaned off or secured
    - They likely aren't getting updates
    - Many of these devices are older and won't get updates

## 7. Aftermarket Devices

### Maastricht University donated an MRI to the Cuban Neurosciences Center:

## Background on Devices and Systems

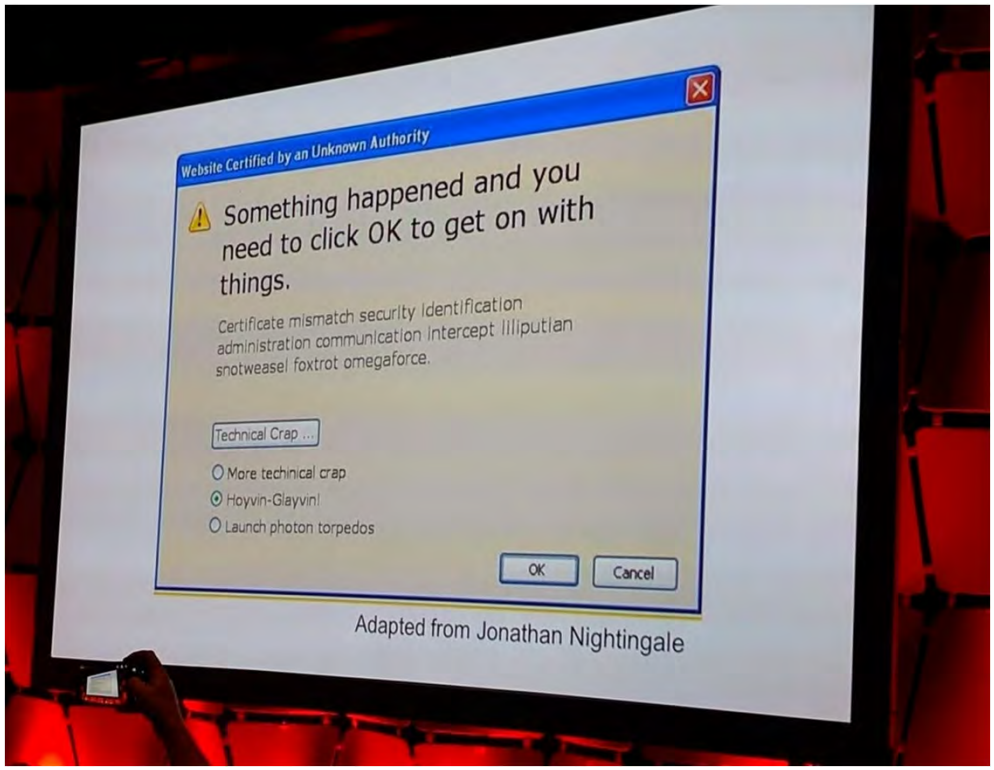
### 7. Aftermarket Devices

- We also need to account for these in M&A and Divestures
  - Do they meet the new corporate standard?
  - Have they been assessed for risk?
  - Most important – if the facility has had financial difficulties, did they cut support?

## Business Drivers

- We have business drivers driving the Internet of Medical Things (IoMT)
  - Shift from Inpatient to Outpatient
  - Need for Monitoring of chronic patients (COPD, diabetes) and compliance
  - Patient Satisfaction/Clinician Communication
  - Population Health
  - Smartphones and Health Apps
  - Fitbits and Consumer Devices

# What does the business see?



## One Weird Trick…

- We're seeing a lot of "one weird trick" marketing from companies offering to sell us equipment to do all the work for us.

## What has happened?

- A number of high-profile incidents have occurred that have demonstrated that medical devices are not secure, and are not meant to be secure.
  - WannaCry
  - Pfizer/Hospira Pumps security issue
  - Ransomware attacks on Windows-based systems
- There is now draft legislation and guidance from the FDA to address these issues that focuses on the development process and vulnerability management
- There are companies and people attempting to resolve these issues using new technologies
  - Blockchain-based tech to verify and validate security and safety of devices across owners by device (Spiritus Partners)

## What has happened?

- There is technology, but there are also business issues to address
- The technology issue is obfuscating the management of devices, and how we can practically plan and manage to have them in the environment
  - Make it so that we have a playbook that non-technical staff can follow and understand and why
- Bridge that last mile with everyone

## Where do we start?

- It starts with a plan
  - Even if you don't have a security team, develop a plan to manage your vendor technology in five areas:
    - Contracts and Language – the rules of engagement
    - Preparation
    - Acquisition
    - Maintenance
    - Disposition

## The five key areas of technology management

# 1. Contracts and Language

- You need to have six core sets of terms in your contracts to address potential security issues:
  - Minimum Security Standards for encryption and supported components
  - Identify how you will be notified of vulnerabilities
  - SLA for notification time/workarounds
  - SLA for patch availability
  - BAA that covers security logging and auditing
    - Who reviews the logs?
  - Identify responsible parties in the contract in writing!

# The five key areas of technology management

## 2. Preparation

- Identify Vendors
- Establish relationships (external)
  - Include other organizations that run this product.
  - Get to know your vendors well and have a relationship.
  - Even if you buy from a GPO, get to know the team
- Establish relationships (internal)
  - Clinical Engineering – esp outsourced managers
  - Consultants
  - Legal/Contract Management
  - Supply Chain (esp. if outsourced!)

# The five key areas of technology management

## 2. Preparation

- Plan to Manage
- Plan for Emergencies/Issues/Downtime/Recovery
- Build standard work that includes service levels
  - Nothing gets done for a CE contractor without a work order (one contract had 6 places that specified this!)
  - Make sure you have a good relationship with the people in charge of CE so you can get work orders issued.
  - Plan for good network security to buy time.
    - **It takes a long time to patch CE equipment due to resource issues.**
    - **Segmenting these devices helps spread the work and make it predictable.**

# The five key areas of technology management

## 2. Preparation

- Identify how you will be notified of vulnerabilities and changes
  - If you are buying used, make sure you can get the patches in the first place and have a reliable resource (read: Not the Pirate Bay) to get them
    - **ECRI, FDA, vendor themselves, etc.**
- Identify testing/downtime processes
- Identify vendor contacts
- Identify resources
- Identify network requirements and how to meet them
  - Build out how to manage segments and devices.
  - Build out how to monitor networks for anomalies

# The five key areas of technology management

## 2. Preparation

- If you're small, consider a managed service to monitor security so you can collect device logs and be alerted to issues.
  - I do not expect most offices to have a SIEM but they have devices. A managed service helps turn those alerts into plans
  - We made recommendations to draft FDA guidance for log files for this reason
  - We look at the SIEM as being critically important as no human being is going to look at log files.
    - **Let AI, ML, and other tech do this for you**
- Get templated statements of work for product security updates and product maintenance

## The five key areas of technology management

### 3. Acquisition

- If you're acquiring used devices, make sure that you still have a plan to manage as if they were new
  - You may have to pay a little extra to reestablish maintenance contracts
  - If you're going through M&A you need to have this in the playbook!
- Follow through on your processes from Preparation

# The five key areas of technology management

## 4. Maintenance

- Develop and execute Standard work for devices as you need to be able to measure staffing levels and manage these devices
- Log and register maintenance/sec updates on these devices
- Wireless Security is going to be key as standards evolve
- Log and register maintenance on your networks just like CE devices
  - We expect that Joint Commission, based on statements that the loss of a wireless network is a patient safety issue, to ask similar questions
- Make sure you have a documented change management program and follow through with it
  - Log device changes to a central registry

## The five key areas of technology management

### 4. Maintenance

- For large-scale upgrades, use Failure Mode and Effects Analysis to map out potential process failures.
- Make sure you involve all parties and communicate well with them when you perform maintenance.
- Yearly risk assessments and risk management plans to discover and address security issues.
- If you bring in tools, make sure they address a real and identified risk!

## The five key areas of technology management

### 5. Disposition

- Erase devices
- Build erasure/refit costs into sale price
- Consider registering devices in a centralized registry so buyer has history

## What have we learned?

- There is a lot more to the backstory of medical devices than just insecure development
- It takes a lot to change multiple decades of development and evolution from serial ports and dedicated lines to 5G
- Even then, we have to manage these devices differently than we have before
- It's not impossible if you have a plan
- A 5 step plan (Contracts, Preparation, Acquisition, Maintenance, Disposition) can help you immensely

## Thank you!

- Questions?
- Contact Info:
  - Mitchell Parker
  - Executive Director, Information Security and Compliance
  - Indiana University Health
  - Email:  Mitchell.parker@iuhealth.org
  - Twitter:  @mitchparkerciso
  - LinkedIn:  https://www.linkedin.com/in/mitch-p-95a9a04/
  - Cell:  215 519 1053

# A

- W

# A

- W

# Strategically Improving Medical Device Security

Mitchell, Parker, IU Health


Indiana University Health

## Purpose of Presentation

- To show how providers are incorporating security into their strategies and using it to improve their security posture

## Background

- I am the Executive Director of Information Security & Compliance (CISO) at Indiana University Health
  - 17 hospitals
  - Hundreds of clinics across the state
  - 34,000+ team members
  - ~600 person IS department

## Team Makeup

- Our team focuses on six key areas:
  - HIPAA/PCI Compliance (Kevin St. Laurent)
  - Third Party Risk Management (Rachel Money)
  - Penetration Testing (Chris Gibson)
  - Standards Compliance (Mitch Parker)
  - Program Management (Noidric Davis)
  - IU School of Medicine (Nick Sturgeon)

## Interfacing

- As part of our strategic focus, we work closely with a number of business partners:
  - Privacy/Legal
  - Government Affairs
  - Compliance
  - Risk Management
  - Regulatory Affairs
  - Emergency Management
  - Physical Security
  - Chief Health Information Officer
  - An ever increasing number of medical device vendors

## Goals

- To use our strategic alliances to work across organizations to assess and address risks at different levels
- To prevent items from going onto the floor without proper risk analysis
- To maintain what we have in good repair
- To effectively plan out lifecycle management for all items on the network
- To effectively communicate our security requirements
- To continue to have great relationships with medical device vendors

## Notes and Words

- Strategic Goals
- Explaining and fitting together items for vendors using common language
- De-mystifying security for vendors – let them know what to do
- Take the confusion out of security – explain what we need
- Explain the goal of a constant review process
- Explain our focus on the processes, not on checking boxes
- Build a virtuous cycle to assess and address risk

## What is our approach?

- We want to work with our vendors to develop security as part of the overall business process
- We don't want to overwhelm you with questionnaires and checkboxes
- We want to be very clear about what we need to demonstrate that you meet our organizational standards and requirements
- We want to work with you and build partnerships – no adversarial relationships
- We don't want to scare our customers, or you – that does nothing to help us
- We want to avoid preventable issues that can affect our patients

## What processes do we use to address this?

- Governance/Intake
- Enterprise Architecture Review
- IT Risk Assessment/Information Security Review
- Privacy Impact Assessment
- Business Associate Agreement
- Internal Policies and Processes
- Internal Review

## What do we expect from medical device vendors?

- Security Contacts
- Realistic Operational Management Tasks and Expectations
- Explanations of Security Management Processes
- Openness into your product development processes
- Vulnerability Management Processes with Excellent Communication
- Privacy and Security by Design
- Network Security by Design

## Governance

- Organizations need to have a gate for purchases that represents a business unit
- Need to make sure that purchases are consistent across organization – reduce variety
- Need to make sure that purchases meet strategic requirements
- Buy only what we need to – efficient spend and allocation of limited resources

## Enterprise Architecture Review

- Yes, this meets our strategic needs, but…
- Does it integrate with what we have?
- Does it integrate with the key systems we use?
- Can we do enterprise provisioning?
- Does it use standard data formats?
- Do we have to reinvent the wheel to fit this in our environment?
- Most Important:  Can we implement security standards at the beginning?
  - Can we segment and run your devices as isolated as possible?

## Information Security Review

- The IT Risk Assessment is only part of this
- We designed it for several main goals:
  - Vulnerability Management – do you do this in a timely manner?
  - Do you continually assess and address issues?
  - Do you incorporate security and privacy by design?
  - Do you update all components, not just your software?
    - I have seen vendors update software and leave the operating systems, database systems, and web servers obsolete
- Comprehensive Review of security practices and procedures
- We will interview CISOs and key security and management leaders
- Do you protect our patients' information to our standards or better?

## Privacy Impact Assessment

- Do you only collect minimum necessary information?
- What data will you be collecting?
- What format is the data in?
- Where will you be storing it?
- How will you be accessing the data?
- Will you be doing any aggregation or de-identification?
  - If so, what is the reason?
- Do you have plans to use our data for any other purposes, even if de-identified?

## Business Associate Agreement

- Legal document that covers requirements, liability, and security details
- We address breach response, data handling, expected insurance amounts, and responsibilities
- We also have Appendix A to discuss security requirements
- As part of that, we broke ours out in detail
  - We discuss certificate management, logging, auditing, provisioning, risk assessments, network design, and vulnerability management
  - Instead of addressing HIPAA as one statement, 14 separate statements in plain language with explanations that are most important

## Business Associate Agreement

- We do this to put these items up front when you sign a deal with us
- We want it well known what we are looking for
- We also want to let people know that we are looking for compliance with the HIPAA Security Rule in detail
- We've found that many of our vendors were not aware of specific requirements, e.g. Cloud Computing, and we need to be detailed in spelling them out

## Internal Policies and Procedures

- Organizations need to have strong policies and procedures
- Need to spell out exactly what responsibilities are and who needs to do them
- Need to be no longer than necessary
- Should have corresponding training with question instrument
- Need to be updated as needed, which may be more than some people are used to
- Need to be well communicated throughout the organization
  - With recorded training instrument answers – OCR looks for this

## Internal Review

- According to the 2017 Online Threat Report, 93% of the data breaches out there were caused by people not taking due care or patching
- According to Phil LaDuke in Entrepreneur Magazine, November 8, 2016:
  - If 80 Percent of Success Is Showing Up Then 20 Percent Is Following up
  - *The excuses are many, but the solution is surprisingly simple*
- We need to make sure that we and our customers follow up and do what is needed to address security issues
- When we present stories of data breaches to leadership, ultimately every case has root causes in lack of preparation or due care

## Internal Review

- We address this by following up
- However, to do this, you need to lay everything out for people to know
  - Clear policies and procedures
    - Explain all requirements and what is needed
  - Good education plan
  - Good intake process
  - Supporting governance
  - Realistic financial expectations and planning
  - ASSET MANAGEMENT - know what you have!

## Internal Review

- As part of these requirements, you design controls tests, just like Internal Audit does
- You review and follow up with your customers
- Get documented evidence of compliance
- Escalate to leadership if not being followed
- If you do this, you address the largest risk

## Now we come to expectations from vendors…

- This is where we discuss what we need to see from medical device companies
- We look at this as going both ways
- If we can get some small improvements here we can greatly improve security

## Security Contacts

- We want to have direct contact with product security teams
- Instead of having a general customer service number, direct lines to security professionals who can address issues
- The goal is to address potential security issues without having to go through several levels of staff members to explain an issue
- This has been a major frustration as security researchers or customers have had to track down people to report vulnerabilities or issues

## Realistic Operational Management Tasks and Expectations

- Time is Money, especially when you have a large operational tail for product maintenance
  - Security work is preventive maintenance
  - We need to budget for time per device to maintain it
  - We need to be realistic as healthcare has limited budgets
    - Either we pay to do it or we pay someone else as part of a work order
    - Large Clinical Engineering outsourcing firms require detailed work orders
    - The front-line staff who implement security remediations do not necessarily need to know

## Realistic Operational Management Tasks and Expectations

- The people who write the work orders or manage Clinical Engineering staff normally do not understand what to do for security
  - If you're lucky, they will call you when they get recall notices
- Therefore, we need to be very clear and circumspect and spell out everything that needs to be done as regular tasks
- Make it so that someone who does not know technology or security can copy and paste them into task lists or work orders
  - Explain that you are being realistic about operational costs and reducing risk
  - This also allows us to design controls tests for following up!

# Explanations of Security Management Processes

- We need to understand how you manage security, prioritize risk, and develop security fixes
- We also need to understand how you expect us to manage them
- As part of managing these devices, we need to understand how to design security in our environments around them
- We need this information to plan security responses based on how you work

## Openness into Product Development Processes

- We want to help you avoid issues or make mistakes
- You also need to understand how the environments you are deploying into will work
- We want you to take these issues into consideration when developing products
- It's our goal to make deployments easy

# Vulnerability Management Processes with Excellent Communication

- It's sometimes really hard to sometimes ascertain what is in a patch and what it does
- We are up against change management where we have to understand what a patch changes and what it does
- We need to understand how long per device remediation will take (remember, non-technical people apply these patches)
- We need to know all that and have it documented for us so that we can communicate the urgency to our stakeholders

## Privacy and Security By Design

- We would like to see you only collect information you absolutely need to do your job and nothing more
  - Think European Union General Data Protection Regulation (GDPR)
    - GDPR requires this!
- We also want security designed in
  - Don't use default passwords
  - Use secure connections
  - Allow us to install our own SSL/TLS certificates and crypto keys
  - Make it easy to manage them

# Privacy and Security By Design

- Security Designed in
  - Make it simple to patch and maintain
  - If it involves a command line, you increase time to maintain and the probability of error
  - Make documentation for patching and maintaining devices as simple as possible
  - Provide human-readable error messages and warnings for issues
    - Codes are for auto mechanics – we need to act quickly and if we have to look up something it leads to confusion
    - Reduce acronyms!

## Network Security By Design

- We need to keep your devices as segmented as possible
- We can no longer assume the risk of having medical devices on the same network as PCs – esp. if running Windows
  - Yes, we are aware of medical devices that have had ransomware
- Segmentation buys us time to patch
- It also can reduce risk from insiders and outsider attacks by only allowing access based on role
- We need to extend this to wireless as well
  - However, we need you to support WPA2-Enterprise to fully support this!

## Conclusions

- We want to work with manufacturers to improve security
- However, the solutions with the highest return are not entirely technical
- Better communication, understanding of processes, and making sure that the right processes exist goes a long way
- Security is about involving the whole organization in resolving business issues

## Thank you!


- Mitchell Parker
- Executive Director, Information Security and Compliance
- IU Health
- Mitchell.parker@iuhealth.org

# What is a Security Information and Event Manager (SIEM), and do I really need one?

Mitchell Parker, IU Health


Indiana University Health

## Purpose of Presentation

- Security Information and Event Manager (SIEM) software works by collecting log and event data that is generated by host systems, security devices and applications throughout an organization's infrastructure and collating it on a centralized platform.
- This session will cover the information provided by basic SIEMs, and if you need a SIEM, what are low-cost solutions.

# Agenda

- History of the SIEM
- What does it stand for?
- Why do we need them?
- What's the Staffing Requirements
- SIEM Features
- Major SIEM Products/Vendors
- Advantages/Disadvantages
- Example Logs/Reports
- Low-Cost/Free Solutions
- Final Tips

## History

- In the beginning, there were logs
- And there were many of them
- UNIX and Windows generate a lot them
- So do web servers
- And they can send them over serial ports or port 514
- Windows can also send them to remote servers
- People wanted to aggregate and analyze them together to understand security events
- They also wanted to store and retain them

## What does it stand for?

- Security
- Information

And

- Event
- Management

System

- A place for your logs and to analyze them

## Why do we need them?

- Log retention of events
- PCI-DSS requirements for log retention
  - PCI requires audit log analysis
  - Retention is state by state on financial data that doesn't have credit cards
- HIPAA requirements for accounting of disclosures and log analysis
  - Six years for Accounting of Disclosures
  - OCR wants logs stored with data
    - Even though states have different retention laws, logs have to be retained as long as data

## Why do we need them?

- DOD requirements for log retention
  - 1 year minimum, 5 for Sources and Methods intelligence (DODi 8500.01 control ECRR-1)
- FedRAMP control AU-11 – The organization retains audit records to provide support for after-the-fact reporting
- FedRAMP control AU-9 – The information system protects audit information and audit tools from unauthorized access, modification, and deletion
- FedRAMP control AU-3(2) - This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system.

## Why do we need them?

- DFARS Regulation 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting requires:
  - (b)(2)(D) – For external cloud services, the contractor must use cloud service providers compliant with FedRAMP requirements
  - FedRAMP controls AU-6 1-10 require the use of automated mechanisms to integrate audit review, analysis, and reporting processes, analyze and correlate audit records, centrally review and analyze audit records, and integrate analysis of audit records with vulnerability scanning info, performance data, and information system monitoring information

## Why do we need them?

- NIST Special Publication 800-171 Revision 2 for non-Cloud services procured under DFARS Regulation 252.204-7012 (b)(2)(i)
- Section 3.3 – Audit and Accountability
  - 3.3.3 – Review and update logged events
  - 3.3.4 – Alert in the event of an audit logging process failure
  - 3.3.5 - Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity
  - 3.3.8 – Protect audit information and audit logging tools from unauthorized access, modification, and deletion

## Why do we need them?

- You cannot meet DOD requirements doing this manually
- Given event volumes and requirements, there is no way to accurately do this manually as it requires normalizing and analyzing events
- There is also no way to do this given the volume of events that servers can generate, which are in the millions
- By the time you do one type of analysis, you will have spent enough resources to buy a SIEM and have them do more
  - Not cost-effective!

## Why do we need them?

- Most platforms overwrite logs when they hit a certain size like Windows or Active Directory
- Need to correlate events across multiple platforms
  - Correlation is often the only time that you can detect intrusions
- Need to be able to trace paths of events
  - People can forge one set of logs
  - They normally don't make the effort to forge all of them
  - Find errors and inconsistencies to identify possible events

## Very practical reasons why we need them

- Need to be able to see when people logged in and out
  - Your HR department will love you for this one
- Ransomware and other advanced attacks rely on blindness to actions
  - Attacks such as UHS, Blackbaud, and numerous others had time between initial intrusion and attacks measured in months
  - No one was watching
- Visibility means that the probability of discovery is much higher
  - If you see something going on you're going to do something
  - If no one is watching or the alarms then you might as well have nothing because you do

## What's the staffing requirements?

- Despite what many vendors will tell you, you will need someone monitoring its health at least part-time
  - There is no such thing as set and forget.  Whoever tells you this lies.
- You will also need to make sure to set timelines to resolve issues and events
- You need to check to make sure all your log sources work and get alerted if they do not
- You also need to check to make sure logs are being ingested and processed correctly
  - One wrong log file and you're out

## What's the staffing requirements?

- You need to check to make sure that you are not getting too few or too many alerts
  - Don't let default settings overload you and cause alarm fatigue
  - Large attacks have succeeded by hiding in millions of events that default SIEM settings have covered up
- Also need to keep the SIEM and underlying systems secure
  - Despite it being a security tool, it's a one-stop shop for information
  - And intelligence on what really runs or doesn't on your network

## SIEM Features

- Integrate logs from many sources
  - AV
  - EDR
  - Active Directory
  - Windows Event Logs
  - Linux/UNIX Syslog
  - Network security devices such as firewalls and IDS/IPS
  - Authentication Logs
  - Storage Area Network
  - Virtual Private Networks
  - Applications

## SIEM Features

- Normalize logs and formats so you can query them and perform analytics
- Integrate threat intelligence feeds to determine if network traffic or stored events match patterns of known attackers
- Match patterns, sequences, and identify specific events that indicate erroneous or malicious behavior
- Identify anomalies
- Report on anomalies
- Store records of logs and potential findings

## SIEM Features

- Feed IDS/IPS and other security systems information on known bad events
  - Be that central hub to centrally arbitrate and distribute
- Ability to develop custom reports on data
- Provide dashboarding and analytics on security events
  - Help you avoid overload and give quick views on events that matter

## What are some of the major SIEM products/vendors?

- ELK Stack (Elastic)
  - Largest Open Source/Free solution
- ARCSight
- McAfee (former Nitro Security)
- Alienvault (AT&T)
- LogRhythm
- QRadar (IBM)
- SolarWinds
- Splunk
  - Probably the largest and most full-featured

## What makes them special? Why do people pay?

- The algorithms
  - Many of the commercial offerings are tuned and come pre-set for different environments
- The data storage
  - They make it easy to expand them
- How they present dashboards of info to people
  - Many have very polished user interfaces
- Ease of use
- The vendor support system
  - Good with less staff

## How do people deploy them?

- On-premises in a rack (people do still have data centers)
- Virtual Machine Image (very common)
- Container (starting to see more of)
- Managed Security Services Provider (MSSP)
  - Let them do most of the work or labor for you
  - Even though they do the hard work you still need to make sure that the systems can send them data
  - They will still deploy Virtual Machines or machines to send events
- In the cloud
  - MSSP's will usually deploy in the cloud

## What are the advantages/disadvantages?

- On-premises advantages
  - Local connection to servers on the same network
  - Disk storage is cheap
    - You pay once for the storage, not recurring like the cloud
  - Can be deployed as a virtual machine or container
  - Don't have to worry about cloud storage charges
  - Don't have to have a continual Internet connection or forwarding server - less complex architecture
  - You don't have metered charges for additional services like firewalls

## What are the advantages/disadvantages?

- On-premises disadvantages
  - Vendors may charge for additional storage
    - This is “special” storage at a 10x markup even though you can buy that drive on Newegg for $200
  - You must buy additional hardware to scale up
  - You may have to buy additional software licenses to scale up
  - You may have to buy licenses to store software
  - You must upgrade and patch yourself
  - Connecting Cloud apps is difficult and opens up potential network holes
    - Many cloud vendors have insecure APIs and don’t use VPNs

## What are the advantages/disadvantages?

- Cloud Advantages
  - Easy to scale out and up
    - Cloud is designed to be elastic
  - Easy to set up
    - Takes 10 minutes to set up in Amazon Web Services
  - Easy to update/upgrade
    - Pushbutton upgrades
  - Ease of connecting Cloud applications
    - No need to set a lot of firewall rules

## What are the advantages/disadvantages?

- Cloud Disadvantages
  - Many of the cloud firewall and IPS systems have metered charges
  - You can get hit by additional costs for processing, memory, additional services, and storage if not careful
    - Storage especially will kill your bottom line if you do not forecast correctly
  - You must upgrade on their schedule
    - Cloud vendors have no interest in having a security system becoming a vulnerability and liability
    - If you don't test upgrades I guarantee future issues

## What are some example logs and reports we need?

- According to the SANS publication, Top 5 Essential Log Reports, Version 1.0 (Source: https://www.sans.org/security-resources/top5-logreports.pdf)
  - Attempts to Gain Access Through Existing Accounts
  - Failed File or Resource Access Attempts
  - Unauthorized Changes to Users, Groups, and Services
  - Systems Most Vulnerable to Attack
  - Suspicious or Unauthorized Network Traffic Patterns

# Attempts to Gain Access Through Existing Accounts

- This report type focuses on several types:
  - Unauthorized logins from outside the network and the number of times they attempted to log in
  - Repeated unauthorized logins from inside the network
  - Logins from workstations or outside by service accounts
  - Logins from foreign countries or different geographic areas
    - Esp. good for finding users using VPNs to log in
  - Logins by normal user accounts to servers other than file servers

## Failed File or Resource Access Attempts

- This is good for finding several types of access patterns:
  - Failed Domain Name System (DNS) transfers
  - Failed DNS recursion attempts
    - May be a sign of cache poisoning
  - Failed accesses to non-existent or restricted web site directories
    - May be a sign of someone trying to probe your systems
  - Failed mail relay events
    - Someone trying to impersonate you and send mail
  - Failed file access
    - Why do they want to see salaries.xlsx?

## Unauthorized Changes to Users, Groups, and Services

- Accounts that have been added
  - Why is the new user r00ted on our file servers?
- Users added to groups
  - R00ted is now a member of Enterprise Admins
- Services added, changed, or deleted
  - R00ted turned off Antivirus
  - R00ted restarted sshd in a new location
  - R00ed added a new service called pwned.exe as SYSTEM

## Systems Most Vulnerable to Attack

- Systems that have not reported in through Event Log that patches were successful
- Systems that have reported in that patches failed
- Vulnerability scanner reports showing vulnerable systems
- Systems that have reported in recent updates/upgrades

## Suspicious or Unauthorized Network Traffic Patterns

- Inbound and outbound pings to non-existent or blocked sites
- Initiated outbound traffic from outside-accessible servers
- Outbound traffic to sites identified by threat intelligence
- Outbound traffic to mail servers, Internet Relay Chat, Virtual Private Networking, or file sharing sites
- Outbound Secure Shell/Secure FTP/FTP traffic
- High bandwidth utilization

## What are some low-cost/free solutions?

- ELK Stack - Open Source ( https://www.elastic.co/start )
- Elastic + LogStash + Kibana
- OSSIM (https://cybersecurity.att.com/products/ossim)
- OSSEC (https://www.ossec.net/)
- Splunk Free (https://docs.splunk.com/Documentation/Splunk/7.2.6/Admin/MoreaboutSplunkFree)
- Apache Metron (http://metron.apache.org/)

## What are the most friendly solutions for non-IT professionals?

- There are numerous user-friendly front ends to ELK Stack
  - The paid version also has great support
- Splunk has a significant community that provides support and code for specific applications

## Final Tips

- If you can't think of who can manage this effectively in 30 seconds, or do not have the budget to hire someone, get a Managed Security Services Provider
  - They can also help you configure/manage your servers
  - Well worth it for smaller businesses that need DOD or HIPAA-level compliance
  - You will need one that is a FedRAMP authorized vendor to do business with DOD according to DFARS Regulation 252.204-7012
    - MSSPs are offsite and can be considered cloud-based
    - GuidePoint, CrowdStrike, and Qualys are authorized

## Even if you go with an MSSP….

- Even though the solution is low-cost, it needs care and feeding like any other IT system
  - Even if its cloud-based you still need to check on and feed source systems
  - You need to forecast your storage needs
  - Calculate how much storage you will need based on the data you have to retain
    - Double it
    - Make sure you have budget for the option you have chosen
    - And that your MSSP contract allows you to expand without killing it!

## Thank you!

- Thank you for your time today
- You can reach out at:
  - Email: mparker17@iuhealth.org
  - Phone/Signal: +1 317 719 5531
  - Twitter: @mitchparkerciso

# Exercise News Release and Information Sheet

# Indiana's Cyber Readiness Advancing Rapidly

Friday, October 1, 2021

If you think about it, protecting a school, hospital, or a city's water supply from a cyberattack is a lot like a football coach drawing up a game plan for playing against the #1 team in the country – every day.

There's game film, playbooks and you always have to account for how you're going to stop the other team's best player from scoring; all the while trying to figure out what else the coach might have up his sleeve. And there's no halftime show to try and adjust to stage a comeback.

That's the challenge facing the State of Indiana in its efforts to continue rapidly moving forward in its mission to further strengthen its cybersecurity resiliency and response.

The progress that's been achieved comes as the State of Indiana and the Indiana National Guard recently hosted two cyber exercises in a partnership with several federal agencies, health care providers, and technology companies, water utility service providers, state, and local government officials, as well as state and federal emergency and law enforcement agencies.

"Conducting these exercises highlights the strength of the cybersecurity structure that exists within the state and underscores the work that's been accomplished over the past three years by

Indiana Governor Holcomb's Executive Council on Cybersecurity with our partners in the military, academic, public and private sectors," said Indiana Department of Homeland Security Executive Director Stephen Cox. "Most importantly, it represents the progress with cyber that's been achieved on behalf of all Hoosiers when we approach cybersecurity as something that is not solved by one entity alone, but by everyone at all corners of the state."

Having a playbook is especially crucial, given the fact there are not only a seemingly endless number of situations in which a cyberattack or incident can occur, but there are all kinds of circumstances and variables that can interfere with a cyber team's strategy for protecting its systems.

**When Water Runs Out…**

A water utility being attacked is not only scary to every city in America, but the reality of it also happening is real.

The Cybersecurity and Infrastructure Security Agency (CISA) has partnered with the State of Indiana and the City of Fort Wayne to exercise how state, federal, mutual aid, and local government would work together in a long-term cyberattack that eliminates the supply of water from the city, with a special emphasis on the secondary effects for the city's hospitals.

As the Cybersecurity Program Director for the State of Indiana, there's no question cybersecurity impacts every aspect of our daily lives. As we've seen with recent cyber incidents – everything from pipelines to water utilities to schools and hospitals – a cyberattack can create substantial effects and damage to our community and our critical infrastructure, disrupting our daily lives and safety.

**When Natural Disasters Hit…**

Following the completion of the tabletop exercise, a second cyber exercise as part of a full-scale functional exercise hosted by the Indiana National Guard for first responders and several military branches as well as search and rescue teams at the Muscatatuck Urban Training Center.

The grounds of the 1,000-acre facility, located in Southern Indiana, is a real city that includes a built-in physical infrastructure, a well-integrated cyber-physical environment, an electromagnetic effects system and human elements. There are more than 190 brick-and-mortar structures with roughly 1.5 million square feet under roof, 1.8 miles of subterranean tunnels, a cave complex, more than nine miles of roads, managed airspace, a 185-acre reservoir, and a cyber live-fire range.

The focus of the Indiana National Guard exercise centered on measuring how federal, state, local and private sectors respond to a devastating earthquake.

"We really need to prepare now for these acts which we've already seen here in Indiana and across the world," said Ron Pelletier, founder and chief customer officer at Pondurance, a cyber security company.  "When natural disasters hit all parts of the world, we are seeing more and

more targeted cyberattacks in those affected areas. Investing now in preventative measures is the best way to avoid situations like that from becoming worse. It comes down to planning to avoid cyber breaches but being prepared to respond."

As emergency and military teams respond to the effects of the earthquake, the Indiana National Guard also tested the additional response of its incident command leadership while the cyber experts from IU Health, Citizens Energy Group, and Pondurance made the efforts more difficult by attacking the water supply in the aftermath.

**It's Not "If" But "When"...**

Pelletier added that Pondurance hopes disaster drills, such as these two, will raise awareness among policy makers to help fund security programs and protocols. "National, state, and community security is truly at risk here, and we need to take action now to preserve it. Waiting for the dam to burst before you repair it is a terrible maintenance strategy, and that's exactly the situation we have here across power grids, water supplies, healthcare, you name it."

Having the ability to draw on the resources and expertise required at a moment's notice to keep people safe in the event of a cyber incident or attack relies on making certain that the state and its partners have a line of communications that's always open to make sure the State of Indiana provides a response that's most effective, regardless of the circumstances.

Many of those who are participated in both state exercises also serve on the Indiana Executive Council on Cybersecurity (IECC). As defined in Executive Order 17-11 from Indiana Governor Eric Holcomb, the IECC is a first-of-its-kind collaboration, whose work as an organization within state government, is responsible for guiding the state's cybersecurity policy, It is comprised of 35 Council members and 250 advisory members, all of whom are subject matter experts represent a wide range of businesses, industries and professions, including education, finance, utilities and insurance, among many others.

The State of Indiana and its partners offer best practices, guides, toolkits, and resources to allow all organizations and critical infrastructures to mitigate, but also prepare for a cyberattack. For more information about the IECC or the State of Indiana's Cyber Strategy, visit www.in.gov/cyber.

For more information about CISA's cybersecurity services and resources, visit www.cisa.gov.

INDIANA NATIONAL GUARD

# Homeland Defender 2021

**Exercise Director:** LTC Robert Brake (INNG)

**Executive Council:** Chief Tom Neal (IN TF1) & LTC Robert Brake (INNG)

**Safety Director:** CSM Ty Benham (INNG)

**Operations Director:** Chief Jay Settergren (IN-TF1)

**Operational Support:** CPT Pemberton (INNG)

**MSEL Directors:** DC Steve Coover (MFD & IN-TF1) & LTC Robert Brake (INNG)

UNCLASSIFIED

INDIANA NATIONAL GUARD

# HOMELAND DEFENDER 2021

POC: LTC Rob Brake

## Exercise Mission

INNG host a Full Scale Exercise from 13-15AUG21 vic MUTC involving local and state resources in order to (IOT) reinforce existing relationships, create new ones and share best practices within the 1st responder community.

## Exercise Purpose

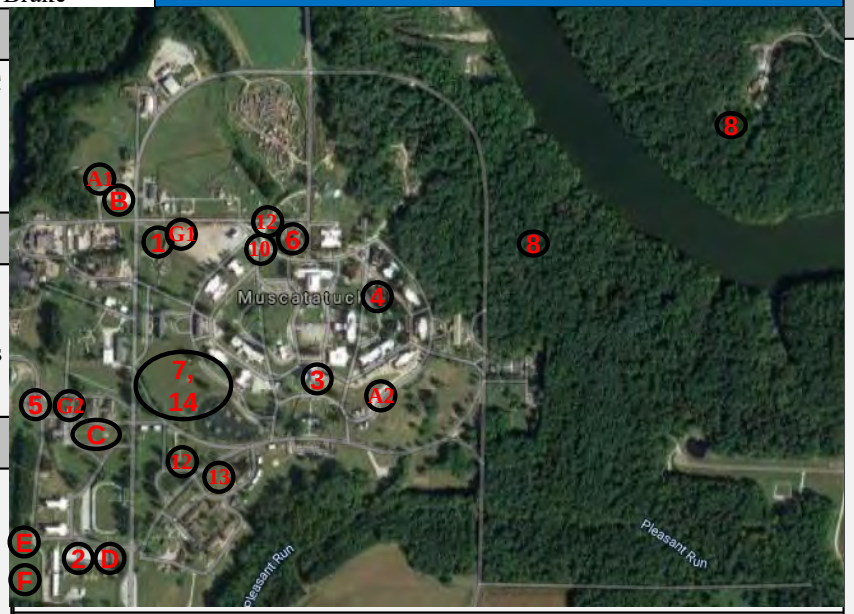
Conduct a joint training event that includes local, state & military partners, focused at the Team level, in order to increase unit/team proficiencies and integration with other 1st responders within the State of Indiana Response Forces.

## Exercise Intent

**Exercise Commander Intent:** Provide a realistic training opportunity for units to collectively train together IOT increase readiness and share tactics, techniques, and procedures via a scalable and nested exercise over a 2 day, weekend exercise. Once completed units, can receive a facilitated AAR based on individual unit training requirements.

**Key Tasks:** Alert & Mobilize, Deploy, Site Occupation, Joint /combined Operations & Redeploy all IAW NIMS.

**End State:** Create a realistic collective exercise from H-hour – OP3, that supports Local and State Inter Agency Integration followed by after action reviews IOT ensure State Partners meet individual and team training objectives, increase readiness and share techniques between Agencies.




## Concept of Operation

A series of earthquakes occur that quickly exceeds local resources requiring assistance from Regional and State Agencies in order to meet lifesaving operational requirements.

As a result multiple agencies and units receive an Alert Orders to Deploy to staging locations. O/O units will move forward IOT conduct Site Occupation & link up with the Incident Management Team (IMT) IOT receive missions for Full Scale Operations. Once units are Mission Complete, they will begin recovery operations and redeploy to home station.

## Operational Lanes:

Lane #1: Initial Command Post & Rail Yard
Lane #2: Unified Command / IMT CMD Post
Lane #3: Hospital Chemical & Radiation
Lane #4: Round Robin Skills Training
Lane #5: Cafeteria Collapse
Lane #6: School Collapse
Lane #7: TF1 Air Load Operations
Lane #8: Lost Personnel WAS
Lane #9: CYBER Ransom
Lane #10: Chaplain Teams
Lane #11: NGRF Alert and Staging Operations
Lane #12: Area Security Operations
Lane #13: Crowd Control Activities
Lane #14: Lifeline Operations

Site A: Staging (Sites 1 & 2)
Site B: MFD & CST CMD Post
Site C: CERFP & TF1 CMD Post
Site D: NGRF CMD Post
Site E: White Cell Team
Site F: Ravenswood Support site
Site G: DECON Sites ( 1& 2)

## Participants/Enablers: 369 (82) BOG -501

CST – 20 (2)
TF1 IN – 6 (15)
CERFP – 208 (5)
CAP – 2
NGRF – 40 (5)
38th CAB – (4)
Ravenswood – (24)
IDHS Dist 8 IMT – 12
127th CB – (2)

MFD – 16 (6)
81st TC – (10)
IOT – 15 (3)
JCSD – 40
UPAD – 6 (2)
ASOS – 4
JFHQ-IN – (4 )

( ) = non-participant / support role

Additional:
Role Players – (50)

IPR #1 10SEP20 → **CDC** 06-08OCT20 CAIN/MUTC → IPR #2 1NOV20 → IPR #3 4DEC20 → **IPC** 2-3MAR21 MS Teams → **MPC** 16-17MAR21 MUTC → **FPC** 11-12MAY21 MUTC → IPR #4 21JUN21 → IPR #5 19JUL21 → **Execution** 13-15AUG21 MUTC

UNCLASSIFIED

# Homeland Defender Key Events Timeline

1-12 AUG 21 Local media reports increased cyber activity to local municipalities

0330 13 AUG 21 – 4.3 MAG Earthquake

13 AUG 21 – HAZMAT call out initiates Rail Yard and Hospital Scenarios (Lanes 1 and 3)

13 AUG 21 – Second Earthquake Occurs causing multiple structure collapses (Lanes 5 and 6)

13 AUG 21 – IC Requests additional resources from JC-EMA (Lanes 2)

13 AUG 21 – State EOC assigns INNG Forces to IC

13 AUG 21 – NGRF arrives to secure govt. center (Lane 12)

14 AUG 21 – Search and Extraction of structure collapses (Lanes 5 and 6)

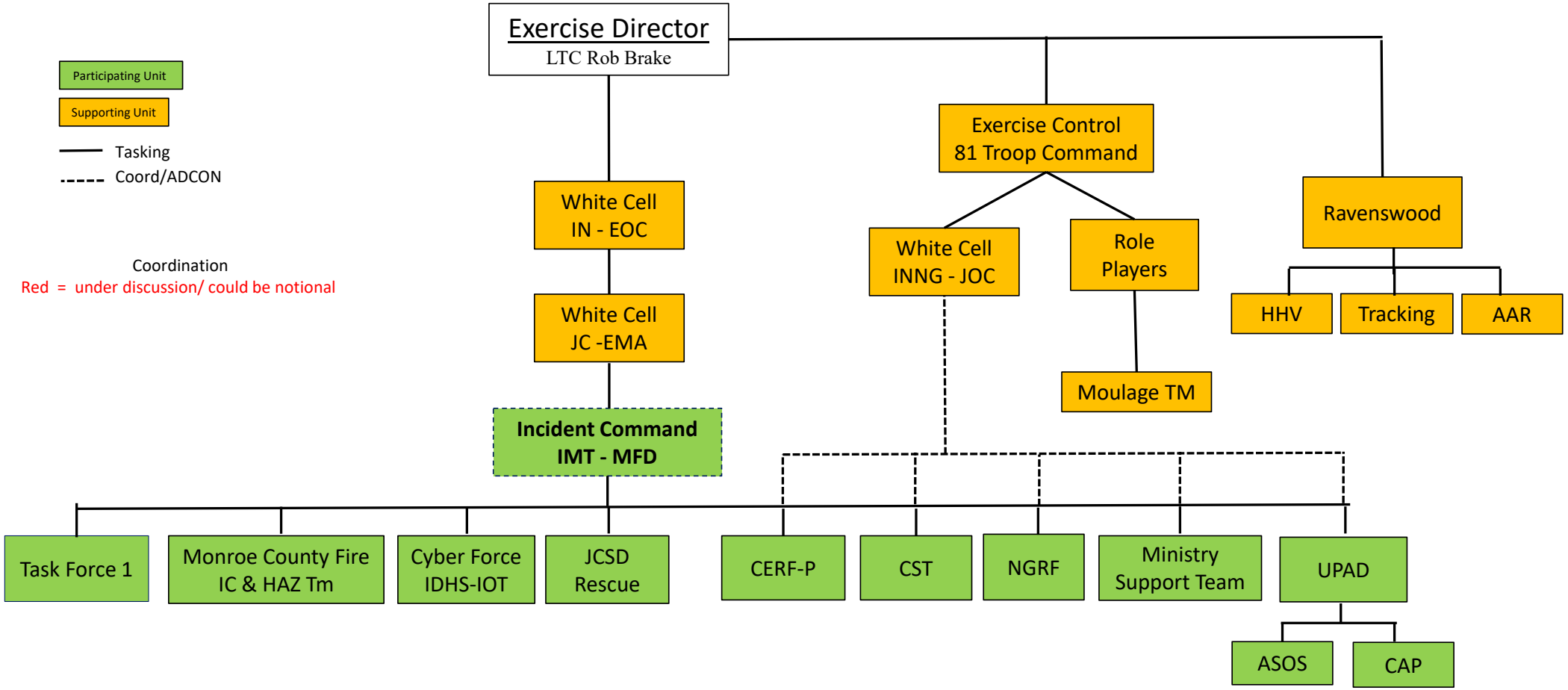
14 AUG 21 – Cyber ransom attack at water treatment facility (Lane 9)

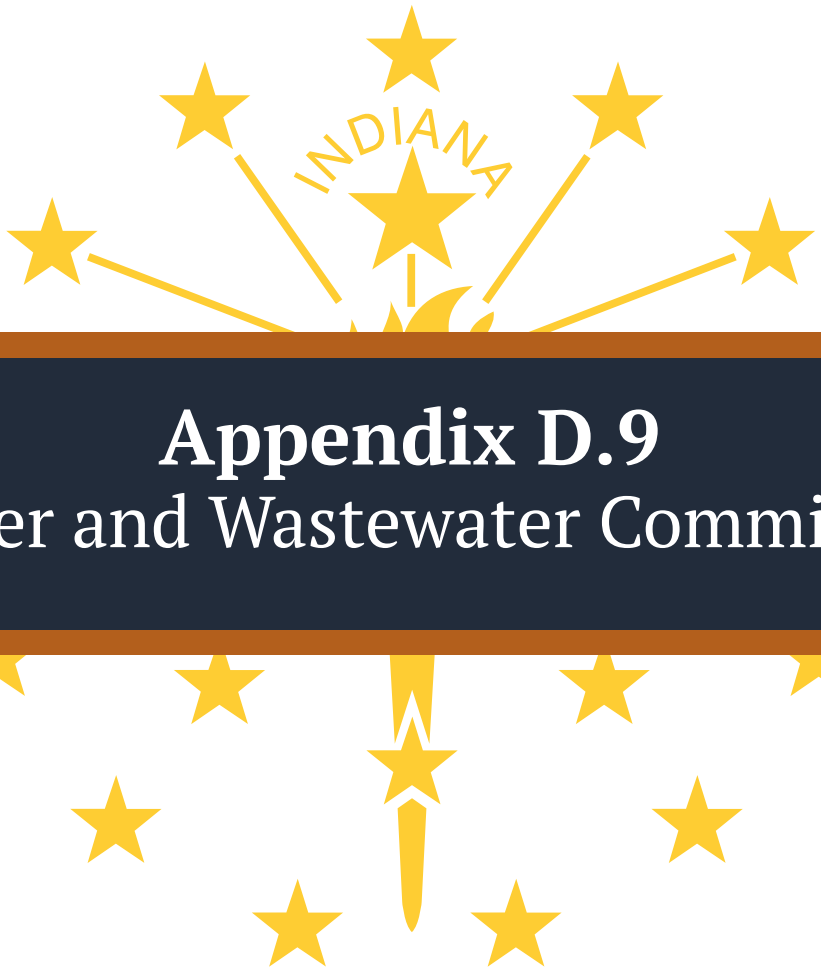
14 AUG 21 – Increase civil unrest at govt. center (Lane 13)

14 AUG 21 – Wide area search for lost personnel (Lane 8)

INDIANA NATIONAL GUARD

# Task ORG

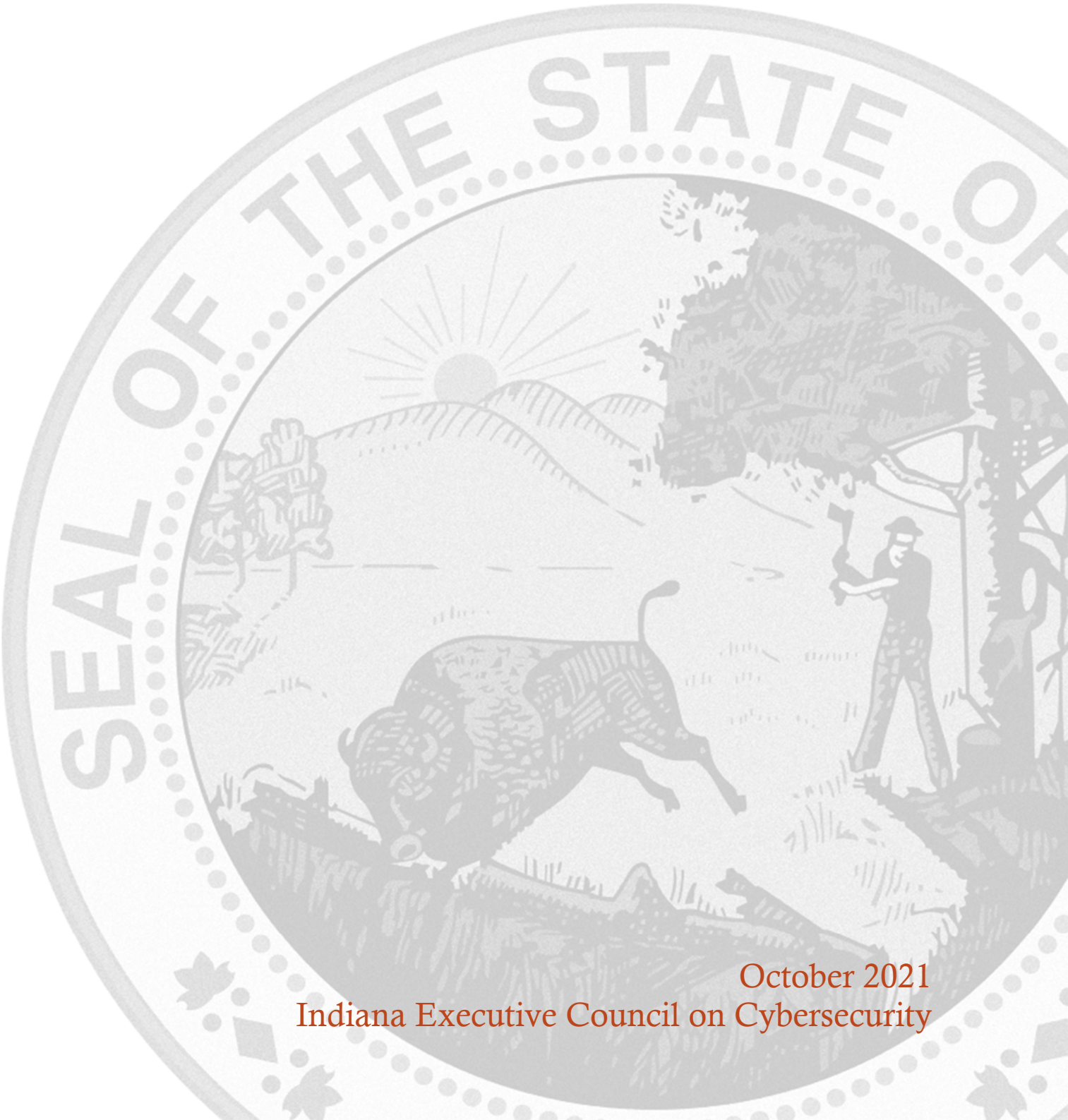





# Appendix D.9
## Water and Wastewater Committee

# WATER & WASTEWATER COMMITTEE STRATEGIC PLAN

Chair: John Lucas
Co-Chair: Martin Wessler




October 2021
Indiana Executive Council on Cybersecurity

# Water & Wastewater Committee Plan

# Table of Contents

# Committee Members

## Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Lucas | John | Citizens Energy Group | Vice President, IT Group | Chair |
| Wessler | Martin | Wessler Engineering | Chairman & CEO | Co-Chair |
| Justice | (Dr.) Connie | IUPUI | Professor | Full Time |
| Redman | Justin | Citizens Energy Group | Manager, Water System Control & Planning | Full Time |
| Moody | Chris | Evansville Water and Sewer Utility | Software Engineer | Full Time |
| Foreman | Jamie | City of Carmel | Drinking Water Regulatory Compliance Administrator | Full Time |
| Bowen | Brandon | Indiana Utility Regulatory Commission | Senior Utility Analyst | As Needed |
| Krevda | Stefanie | Indiana Utility Regulatory Commission | Commissioner | As Needed |
| Funk | Michelle | Indiana Utility Regulatory Commission | Senior Analyst | As Needed |
| Rockensuess | Brian | Indiana Department of Environmental Management | Chief of Staff | As Needed |
| Goodwin | Travis | Indiana Department of Environmental Management | Senior Environmental Manager, Security in Counter Terrorism Coordinator | As Needed |
| Keyler | Dawn | Wessler Engineering, AWWA, InWARN | Project Analyst II, Chair of Indiana Section AWWA Emergency Response Committee, Secretary for InWARN | Full Time |
| Hadley | Ryan | Indiana Utility Regulatory Commission | Executive Director | As Needed |
| Sansing | Ebony | Citizens Energy Group | Executive Coordinator, Information Technology | Full Time |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan.*

For more information, visit www.in.gov/cybersecurity.

# Executive Summary

# Executive Summary

- **Research Conducted**
  - The Water/Wastewater committee conducted research in the following area:
    - Water companies / cyber security contact
    - Training for water companies on cyber security
    - Funding / legislative options for cyber security 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 around cyber security for water companies
  - Lack of risk management plans and action plans for cyber incidents

- **Committee Deliverables**
  - Cyber Contact
  - Cyber Risk Model (Plan) Update
  - Risk Tool
  - Training Plan
  - Cyber Plan Template
  - Cyber Exercise and Response Education

- **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 Indiana American Water Works Association (AWWA) has provided training via the AWWA website
   b. Created and ran the Indiana Crit-Ex exercises in 2015.
   c. Established an Indiana Water/Wastewater Cyber Security Training program (Pilot)

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 cyber security 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 13956 – Modernizing America's Water Resource Management and Water Infrastructure
   b. Indiana Senate Enrolled Act 362, 2018
   c. America's Water Infrastructure Act of 2018 (AWIA)

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.**
   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 AWWA resources and webinars/seminars.

8. **What does success look like for your area in one year, three years, and five years?**
    a. One year
        - Practical cyber training exercises (Muscatatuck, etc.)
        - Implement cyber training and assessment pilot program with Indiana Section of AWWA
    b. Three years
        - Cyber training assessments and developing cybersecurity plans for small and medium size water/wastewater utilities
        - Federal and/or State Financial support for cyber security improvements at small and medium size water/wastewater utilities
        - State Standards for cybersecurity
    c. Five Years
        - All water/wastewater utilities in Indiana participated in cyber training and assessments and have developed and implemented cybersecurity plans.

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 preparedness

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. Approximately 500 water/wastewater utilities and companies.
    b. Workforce at small and medium size utilities is predominantly operator based with limited to zero cyber security personnel
    c. Workforce at large municipalities and utilities typically have IT departments with cyber personnel but may not be dedicated entirely to the utility.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. Crit-Ex; Cyber Gym; Grow the number of companies, whose corporate headquarters are located in Indiana. This creates the need for cyber security companies.

12. **What are your communication protocols in a cyber emergency?**
    a. Vary by utility

13. **What best practices should be used across the sectors in Indiana?**
    a. Risk based templates for evaluating cyber risk (NIST based)
    b. AWWA Cybersecurity Guidance and Assessment Tool
    c. EPA Vulnerability Self-Assessment Tool (VSAT Web 2.0)

# Deliverable: Cyber Contacts

# Deliverable: Cyber Contact

## *General Information*

1. **What is the deliverable?**
   a. The deliverable will be to update a cybersecurity contact list for water and wastewater organizations. The list, developed by the Water/Wastewater Committee in 2018, is in the form of a database that will be regularly updated with contacts specific to each organizations cybersecurity initiatives. This database will work in concert with existing databases that house additional information for the individual organizations business structure. An added field will complement the focused contact information that exists and provide a direct contact for cyber related information. The Safe Drinking Water Information System (SDWIS) contains information about public water systems managed by Indiana Department of Environmental Management (IDEM). IDEM will be modified to include the added field for the 'Plant SCADA Manager'.

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?**
   a. The result will be a regularly updated database of cybersecurity contacts for the water/wastewater organizations in the state. This database will be managed and updated at regular intervals by the organizations through the existing update process. This contact will dispense specific focused information to the correct individual of each organization.

6. **What metric or measurement will be used to define success?**
   a. An updated database that establishes a field for cyber security contacts. Cybersecurity contacts are updated by the individual organizations of medium and large operators.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☒ 2025+

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 cyber security related information sharing.
   b. Other industry organizations like Indiana Water/Wastewater Agency Network (INWarn), AWWA, 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. Indiana Department of Environmental Management (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

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 required to supply the contact information.

# *Implementation Plan*

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

☐ One-time deliverable
☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Modify IDEM SDWIS Database to include new field | IDEM/Travis Goodwin | 100 | 11/2017 | IDEM completed database modifications |
| Request organizations to submit 'Plant SCADA Manager' to IDEM for updates | IDEM | 100 | 1/2018 | Requests made to organizations. Awareness shared by partnering organizations INWarn, AWWA |
| Update database upon receipt of information | IDEM | 100 | 2025 | IDEM recently completed the regular update prior to inclusion of the 'Plant SCADA Manager'. Next regular update cycle anticipated to have better return. |

## Resources and Budget

**15. Will staff be required to complete this deliverable**?

☒No ☐ Yes

**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 |
|---|---|---|---|---|---|---|
| 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 | | |

**17. What is the greatest benefit of this deliverable?**

a. State organizations like IDEM, DHS, IURC, and ISP will have the right contact for cybersecurity related information sharing.
b. Other industry organizations like INWarn, AWWA, IWEA will also be able to information share using the database.

**18. How will this deliverable reduce the cybersecurity risk or impact? What are 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, awareness specific to Indiana's water and wastewater sector.
b. Benefits also include supporting organizations will have the right individual to share information and reach out for information that may support other organizations or the cause.

**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 'Plant SCADA Manager' 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?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. 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?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. 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, IWEA

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

☒No ☐ Yes

a. Critical contact information should not be shared. IDEM should manage contact information requests specific to critical infrastructure.
b. Reference Indiana Code 5-14-3, where several references are made to excepted from disclosure the names and contact information of individuals.
c. More 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. None

## *Evaluation Methodology*

**Objective 1:** Indiana Department of Environmental Management maintains a cybersecurity contact information for 85 percent of Indiana water and wastewater organizations to be reviewed 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
☐ Quantifiable Measurement
☐ Other

# Deliverable: Cyber Risk Model (Plan)

# Deliverable: Cyber Risk Model (Plan) Update

## *General Information*

1. **What is the deliverable?**
   a. The deliverable is to review and update the 2019 deliverable of 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?**
   ☐ 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?**
   a. The result will be a standard method for organizations with Indiana and the U.S. 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 template to enable completion of an assessment within one day for organizations with varying business structures and size.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Water and wastewater (W/WW) 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 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. 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 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?**

☐ One-time deliverable

☒ Ongoing/sustained effort

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Questionnaire | Justice and W/WW Group | 100 | 4/30/2022 | |
| Risk Assessment Documentation | Justice | 100 | 4/30/2022 | |
| Risk Assessment Onsite Beta Test | Justice | 100 | 4/30/2022 | |
| Risk Assessment Report | Justice | 100 | 6/15/2022 | |
| Review Assessment Results with W/WW Group | W/WW Group | 100 | 6/15/2022 | |
| Rewrite Questionnaire/Report if needed | W/WW Group | n/a | 6/15/2022 | |

### Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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 |
|---|---|---|---|---|---|---|
| W-WW 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 Wastewater | Expertise | 0 | 0 | N/A | N/A | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. State of Indiana and AWWA will have a risk assessment model for water and wastewater utilities. This model allows a statewide standard and measurement tool to assist each individual water and wastewater utility with measuring their risks and the state a method to measure statewide risks.
b. Regularly conducted risk assessments close cybersecurity vulnerabilities and mitigate before the vulnerabilities are compromised 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 action plan for each utility, the risk model will allow the water and wastewater companies to reduce 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 a proper SETA program can 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.
   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. 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?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. The AWWA has developed a cyber self-assessment tool that is available to any company nationwide that can be used by any W/WW utilities. The AWWA has developed an updated online cyber security tool which incorporates the risk tool developed by the W/WW committee. This nationwide tool will be utilized going forward by Indiana utilities.

## 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?**

☐No ☒ Yes

a. Water and Wastewater cybersecurity committee will work with the Architectural and Industrial Maintenance (AIM) committee, IDEM, and the Indiana Finance Authority (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. Indiana AWWA, IDEM, State of Indiana Cybersecurity Program Director

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. 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, Indiana Office of Technology (IoT), IDHS, IDEM.

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

☐No ☒ Yes

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

a. Defer to State of Indiana Cybersecurity Program Director

## *Evaluation Methodology*

**Objective 1:** The Water/Wastewater Committee and partners will review and update the Cyber Plan Template for Indiana water/wastewater companies in 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

**Objective 2:** Make the updated Cyber Plan Template available online or on water/wastewater utilities by in 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: Risk Tool

# Deliverable: Risk Tool Update

## *General Information*

1. **What is the deliverable?**
   a. Review the 2020 deliverable of 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 as it is incorporated into the training deliverable. 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?**
   ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☒ In-progress 75% ☐ Not Started

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. 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. The Indiana W/WW cybersecurity assessment has been incorporated into the AWWA Cyber Security Tool that is available to all Water Utilities in the U.S.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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 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. 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 will 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) is in 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?**

☐ One-time deliverable

☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review and modify initial documents for accuracy | | 100 | TBD based on funding | |
| 2 RA with IoT to establish technical standards | | 100 | TBD based on funding | |
| Questionnaire | Justice/W/WW Group | 100 | TBD on project plan | NIST CSF/AWWA |
| Review Questionnaire | W/WW Group | 100 | TBD on project plan | |
| Risk Assessment Scoring Matrix | Justice | 100 | TBD on project plan | |
| Review of Risk Assessment Scoring Matrix | W/WW Group | 100 | TBD on project plan | Output score and where entity ranks in relation to others. Mitigation recommendations. Training needed. |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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. Connie Justice | Risk Assessment Content | 0 | 0 | | N/A | |
| Programmers | Programming expertise | 80,000.00 | No Response | AWWA | N/A | |
| IoT | Expertise | 0 | TBD | | N/A | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Speed consistency, ease of use, the ability of water/wastewater companies to conduct without third party support.
b. The ability to automate the risk assessment will allow for
   i. Ease of use
   ii. Uploading data from risk assessment to a repository
   iii. Data can be used as a baseline for measuring effectiveness of program

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

a. More utilization since local Water or Wastewater utilities can use the tool to establish the utilities' cyber risk profile.
b. 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.

**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. Cyber Risk Tool available online at AWWA.org website.

**21. 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

**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?**

☒No ☐ Yes

## Other Implementation Factors

**23. 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

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

☒No ☐ Yes

**25. 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

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

a. IDEM, State of Indiana Cybersecurity Program Director

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. 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)?**

☐No ☒ Yes

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

a. State of Indiana Cybersecurity Program Director

## *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** Make tool available to 80 percent of Indiana AWWA members on AWWA.org for use by Indiana W/WW companies within 12 months of launching.

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. Pilot Training has been developed. Waiting on funding to roll out to the State.
   ☐ 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?**
   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 be able to quantify both their absolute gap, but also their growth, or lack thereof over each period.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

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. The committee lead will work with the Cybersecurity Program Director to define other sectors and/or committees that might have 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. Indiana AWWA, IFA, IDEM

12. **Who should be main lead of this deliverable?**
    a. Dr. Connie Justice 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?**

☐ One-time deliverable

☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Develop project plan | Training Working Group and W/WW Committee | 100 | TBD based on funding | |
| Develop roles by job function | Training Working Group and W/WW Committee | 25 | TBD on project plan | |
| Develop framework of skills required of each role within entity | Training Working Group and W/WW Committee | 50 | TBD on project plan | |
| Coordinate with industry associations for distribution and collection of survey | Training Working Group/W-WW Committee | 75 | TBD on project plan | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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. State of Indiana and AWWA skills assessment model for water and wastewater utilities. Allows a statewide standard and measurement to assist each individual water and wastewater utility with measuring their skills gap and the state with measurement of statewide training needs.
b. Regularly conducted skills assessments close cybersecurity training gaps and mitigate vulnerabilities before they are compromised. These assessments allow the sector to understand their cybersecurity skills gap.

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

a. Along with action plan for each utility, the risk model will allow the water and wastewater companies to reduce 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 a proper SETA program can 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.

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

a. Along with action plan for each utility, the risk model will allow the water and wastewater companies to reduce 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) so a proper SETA program can 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.

**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 be able to quantify both their absolute gap, but also 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. 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?**

☒No ☐ Yes

**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?**

☒No ☐ Yes

## 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**?

☐No ☒ Yes

a. Water W/WW 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. Support by Indiana AWWA

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

a. Indiana AWWA, AWWA, IFA, IDEM

**27. Can this deliverable be used by other sectors**?

☒No ☐ Yes

i. This risk assessment can be modified slightly to used by other sectors

## Communications

---

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

a. Indiana water and wastewater companies, Indiana 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)?**

☐No ☒ Yes

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

a. Can use this training to communicate about new cyber reporting law and outreach to local government technology directors

## *Evaluation Methodology*

**Objective 1:** Water/Wastewater Committee develop an initial training plan by June 2021 and full training plan within three months 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

**Objective 2:** Seventy percent of Indiana water and wastewater companies incorporate the training plan as a part of their operational resources within 24 months of deployment of 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 – Update

## *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 cyber security 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 establish of their specific plan in order to comply with SEA 362.

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?**
   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.

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?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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 and 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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review of cybersecurity plan template by appropriate State Agencies | John Lucas | 25 | 1/1/2022 | |
| Finalized cybersecurity plan template for distribution updated version by IDEM. | IDEM, IFS, IDHS, W-WW committee | 0 | 3/1/2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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 |
|---|---|---|---|---|---|---|
| W/WW 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?**

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 are 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 cyber-attack 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?**

☒No ☐ Yes

**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?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. Water and 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, State of Indiana Cybersecurity Program Director

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. 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 wastewater 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)?**

☐No ☒ 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 and partners will distribute the updated Cyber Plan Template to 50 percent of Indiana water and wastewater companies through a variety of methods (including virtual) by March 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: Water/Wastewater Exercise and Response Education

## *General Information*

1. **What is the deliverable?**
   a. The Water and Wastewater Committee will assist in two tabletop exercises in 2021 to simulate disasters and cyber-attacks across Indiana. These will be open to IECC members, water and wastewater partners, and Indiana healthcare organizations. The first exercise will be run by the IECC and may include members of the Water ISAC, CISA, INWarn, the City of Fort Wayne, etc.. The second exercise will be run with the National Guard at Muscatatuck Urban Training Center and will involve real-life simulations using that facility. Additionally, taking lessons learned and resources from both exercises to develop a free virtual water and wastewater workshop.

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?**
   a. The goals of these exercises are to:
      - Simulate current cyber-attacks within a safe environment to determine opportunities for improvement
      - Provide information on current capabilities and strengths
      - Give a gap analysis of where to improve and why

6. **What metric or measurement will be used to define success?**
   a. Completion of the exercises
   b. After-action report with areas for improvement

7. **What year will the deliverable be completed?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. The IECC, participating water/wastewater organizations, recipients of the report, the Indiana National Guard, and other participating organizations would and have benefitted from this.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. The cybersecurity resources from the IECC, IOT, and National Guard overlapped with federal resources and AWWA, INwarn and Water-ISAC.

## 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 the IECC committee at large on planning one of these, along with the National Guard, CISA, and IoT.

**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 will need to work with IOT, the National Guard, CISA, and HHS/HSCC to complete this.

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

a. State of Indiana Cybersecurity Program Director

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

a. Based upon the 2021 challenges with delivering both tabletops, it comes down to resource and time availability to plan out the scenarios. We also need time at Muscatatuck to effectively plan out the scenarios using their resources and planning.

# *Implementation Plan*

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

☐ One-time deliverable
☒ Ongoing/sustained effort

## Tactic Timeline

**INCyber CISA Exercise – August 11, 2021**

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Prepare with planning partners in initial, mid, and final planning meetings | USDHS CISA and IECC partners | 100 | Jan-July 2021 | |
| Hold Exercise | USDHS CISA and IECC partners | 100 | Aug. 11, 2021 | |
| Review AAR | Cybersecurity Program Director and USDHS CISA | 100 | October 2021 | |

**INNG Homeland Defender Exercise – August 13, 2021**

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Prepare with planning partners in initial, mid, and final planning meetings | INNG and IECC partners | 100 | Aug. 2021 | |
| Initiate cyber IR component | INNG and IECC partners | 100 | Aug. 2021 | |
| AAR | INNG | 50 | TBD | |
| Develop a W/WW workshop to hold virtually | IECC Partners | 100 | October 2021 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|---|
| .5 | .5 | Planning | | State of Indiana – INNG exercise planning | N/A | |

**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 |
|---|---|---|---|---|---|---|
| Web Conferencing Platform | Needed to host the first tabletop exercise | | | | | |
| Muscatatuck Computing Resources | Needed for real-life simulations of IoT | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. The greatest benefit is the production of quantitative results and action plans that detail opportunities for improvement and areas where organizations can take steps to improve.

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

a. This deliverable reduces the risk and impact by providing exact steps and processes organizations can take to reduce them immediately based on the exercise.
This can potentially save organizations up to millions of dollars, by allowing them to focus on more immediate threats to their people, processes, and technologies during an exercise.

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

a. We will not be able to simulate current cyber threats in an environment designed to identify issues for remediation. Organizations within Indiana would not be able to identify and address these threats and dependencies, and not be able to appropriately act if one of these events occurs.

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

a. Success is the completion of the exercise itself. The metrics used to measure success will be the after-action items that we need to follow up on to address issues discovered during the exercises themselves. The baseline is based on the issues discovered, and the number is proportional to the degree of the 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?**

☒No ☐ Yes

a. Indiana is the only state that we are aware of that has involved federal and non-profit agencies, along with the National Guard, to the degree that we have in these exercises.

**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?**

☒No ☐ Yes

## Other Implementation Factors

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

a. Availability of resources at Muscatatuck to help plan out and develop the exercises there.
b. Availability of IECC resources to help plan out and develop the IECC exercise

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

☒No ☐ Yes

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

a. Availability of IECC members and partners to help plan out and develop the exercise

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

a. We have been working with the State of Indiana Cybersecurity Program Director, David Ayers, healthcare partners, federal water/wastewater partners, as well as local, state, and federal partners.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

## Communications

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

a. We would notify the entire IECC community and all Indiana water/wastewater organizations to participate in an online training regarding what was learned from the exercises.

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

☐No ☒Yes

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

a. Since this is such a unique event for the state of Indiana, there will be media and conference opportunities to present this deliverable.

## *Evaluation Methodology*

**Objective 1:** IECC Water and Wastewater Committee and partners will participate in USDHS CISA Exercise in August 2021.

*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 and Wastewater Committee and partners will participate in INNG Hoosier Defender in August 2021.

*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 partners, develop a water/wastewater virtual workshop and launch by October 2021.

*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:** Promote virtual workshop that results in at least 100 registrants by October 2021.

*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

- Cyber Plan Template 1.0
- INNG Hoosier Defender Information Sheet
- Virtual Workshop

# Cyber Plan Template 1.0

# 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 |
| 6/29/2018 | 2.0 | Lucas |

| | | |
|---|---|---|
| 7/10/2018 | 2.1 | Third Draft – 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 | Modifications – Connie Justice |
| 9/6/2018 | 3.1 | Fourth Draft – Connie Justice |
| | | Modifications – Connie Justice, John Lucas, Steve Berube, Jamie Foreman, Jon Weirick |
| 10/22/2018 | 4.0 | Connie Justice |
| 10/23/2018 | 4.1 | Connie Justice |
| 12/15/2018 | 4.2 | Connie Justice |
| 1/3/2019 | 4.3 | Connie Justice |

## 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** |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |

# iv. TABLE OF CONTENTS

# 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.

# 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 INSTRUCTIONS

### HOW TO USE

The Cybersecurity Plan Checklist (the checklist) is designed to check off the plan checklist items as you complete them or if you have them completed already you can check off the item.

Each link next to the check box will take you to the page with further explanation of the checklist item with links to example forms.

### EASE OF USE

The checklist is designed to be easy to use, however, if you have no background in cybersecurity it is recommended that you attend training sessions and attain help with the checklist.

### CHECKLIST DOCUMENTS

The checklist and documents created are living documents and should be updated on a regular basis, when systems or people change, or on a periodic basis.

# Cybersecurity Plan Checklist

## Identify

- [ ] Identify Organization Security Lead
  Identify an organization security lead for you company
- [ ] Classify data
  Identify mission critical data assets and classify data assets in order of importance. Identify personnel responsible for data asset/s
- [ ] Identify assets
  Identify Mission Critical Technology Assets
- [ ] Security policies
  A document that states in writing how a company plans to protect the company's physical and information technology (IT) assets
- [ ] Risk Assessment
  Execute a cybersecurity risk assessment to identify vulnerabilities in business and industrial control mission critical systems
- [ ] Risk Management Strategy
  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

## Protect

- [ ] 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
- [ ] Access Controls
  Granting access and privileges to systems, resources or information needed.
- [ ] Securing Network and Cloud
  Ensure secure communications and multifactor authentication are setup between the business and cloud providers
- [ ] Authentication Policy
  Multifactor-authentication should be used; a passphrase should be used; unique passwords for separate confidential accounts.
- [ ] Data Security
  Protect business data
- [ ] Information Protection
  Data should be protected by proper backups and testing. Proper destruction, incident response, disaster recovery, and business continuity plans in place.
- [ ] Maintenance
  Equipment maintenance/replacement program established
- [ ] Protective Technology
  Storage media management; centralized logging; Service level agreements with third party vendor; and system hardening based on criticality of systems
- [ ] Physical Access
  Physical access limited; procedures to access buildings and server rooms; and no physical plugging into network

## Detect

- [ ] Anomalies and Events
  Device to identify malicious activity (intrusion detection system (IDS)) should be implemented. Logs should be used to notify of failed logins and malicious behavior.
- [ ] Continuous Monitoring
  Web filtering and patching should be used to monitor unauthorized activity.
- [ ] Detection Processes
  Register for cybersecurity alerts and advisories from water sector and government partners to be aware of new vulnerabilities and threats. Segment ICS network from business network. Restrict access of ICS network to internet unless needed.

## Respond

- [ ] Response Planning
  A security and response program should be established to ensure staff is aware of security policies and incident response/notification procedures
- [ ] Respond Communications
  List of primary and backup contacts
- [ ] Analysis
  Investigate incidents, logs, and vulnerability systems; establish a digital forensics program
- [ ] Mitigation
  Contain incidents; mitigate incidents, or accept risks
- [ ] Respond Improvements
  Incorporate lessons learned; update response plans

## Recover

- [ ] Recovery Planning
  Policies and procedures for system instantiation/deployment should be established to ensure business continuity
- [ ] Recovery Improvements
  Incorporate lessons learned from response plans and update response plans
- [ ] Recovery Communications
  Primary and backup contacts for personnel or vendors; points of contact for reporting a cyber incident and requesting assistance with response and recovery

# 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

## 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

## 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.

### 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).

### 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.

## 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.

## 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.

### *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

# 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 |

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 |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

# 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

# 8 EXHIBIT 4: WATER WASTE WATER RISK ASSESSMENT (TO BE DELIVERED)

# 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.

# 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

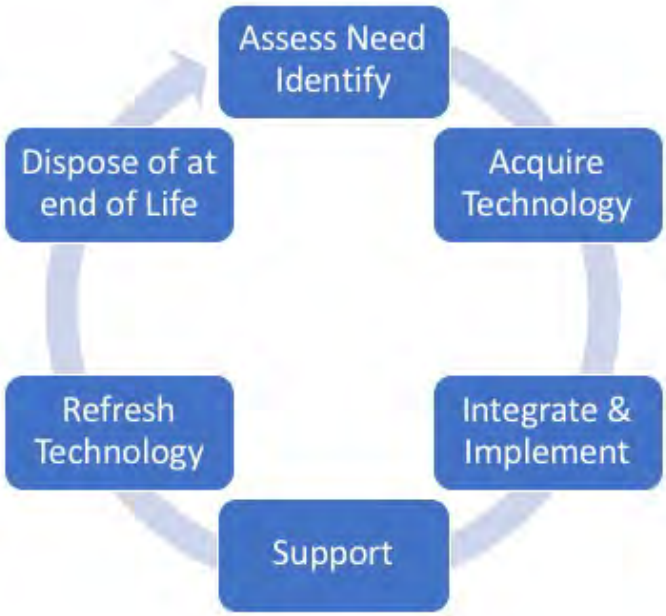
systems. Operational systems and Business systems should reside on two separate physical networks separated by firewall devices.

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 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.

# 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

# 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** | | | |
| | **INWARN Chair** | | | |
| | **State Emergency Management Agency** | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# 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.
[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.]

# INNG Hoosier Defender Information Sheet

INDIANA NATIONAL GUARD

# Homeland Defender 2021

**Exercise Director:** LTC Robert Brake (INNG)

**Executive Council:** Chief Tom Neal (IN TF1) & LTC Robert Brake (INNG)

**Safety Director:** CSM Ty Benham (INNG)

**Operations Director:** Chief Jay Settergren (IN-TF1)

**Operational Support:** CPT Pemberton (INNG)

**MSEL Directors:** DC Steve Coover (MFD & IN-TF1) & LTC Robert Brake (INNG)

UNCLASSIFIED

INDIANA NATIONAL GUARD

# HOMELAND DEFENDER 2021

POC: LTC Rob Brake

## Exercise Mission

INNG host a Full Scale Exercise from 13-15AUG21 vic MUTC involving local and state resources in order to (IOT) reinforce existing relationships, create new ones and share best practices within the 1st responder community.

## Exercise Purpose

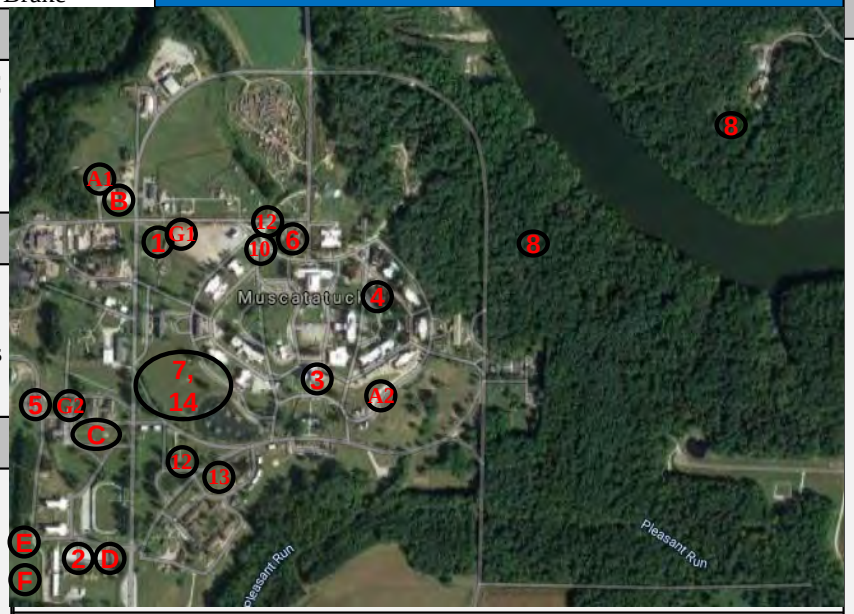
Conduct a joint training event that includes local, state & military partners, focused at the Team level, in order to increase unit/team proficiencies and integration with other 1st responders within the State of Indiana Response Forces.

## Exercise Intent

**Exercise Commander Intent:** Provide a realistic training opportunity for units to collectively train together IOT increase readiness and share tactics, techniques, and procedures via a scalable and nested exercise over a 2 day, weekend exercise. Once completed units, can receive a facilitated AAR based on individual unit training requirements.

**Key Tasks:** Alert & Mobilize, Deploy, Site Occupation, Joint /combined Operations & Redeploy all IAW NIMS.

**End State:** Create a realistic collective exercise from H-hour – OP3, that supports Local and State Inter Agency Integration followed by after action reviews IOT ensure State Partners meet individual and team training objectives, increase readiness and share techniques between Agencies.




## Concept of Operation

A series of earthquakes occur that quickly exceeds local resources requiring assistance from Regional and State Agencies in order to meet lifesaving operational requirements.

As a result multiple agencies and units receive an Alert Orders to Deploy to staging locations. O/O units will move forward IOT conduct Site Occupation & link up with the Incident Management Team (IMT) IOT receive missions for Full Scale Operations. Once units are Mission Complete, they will begin recovery operations and redeploy to home station.

## Operational Lanes:

Lane #1: Initial Command Post & Rail Yard
Lane #2: Unified Command / IMT CMD Post
Lane #3: Hospital Chemical & Radiation
Lane #4: Round Robin Skills Training
Lane #5: Cafeteria Collapse
Lane #6: School Collapse
Lane #7: TF1 Air Load Operations
Lane #8: Lost Personnel WAS
Lane #9: CYBER Ransom
Lane #10: Chaplain Teams
Lane #11: NGRF Alert and Staging Operations
Lane #12: Area Security Operations
Lane #13: Crowd Control Activities
Lane #14: Lifeline Operations

Site A: Staging (Sites 1 & 2)
Site B: MFD & CST CMD Post
Site C: CERFP & TF1 CMD Post
Site D: NGRF CMD Post
Site E: White Cell Team
Site F: Ravenswood Support site
Site G: DECON Sites ( 1& 2)

## Participants/Enablers: 369 (82) BOG -501

CST – 20 (2)
TF1 IN – 6 (15)
CERFP – 208 (5)
CAP – 2
NGRF – 40 (5)
38th CAB – (4)
Ravenswood – (24)
IDHS Dist 8 IMT – 12
127th CB – (2)

MFD – 16 (6)
81st TC – (10)
IOT – 15 (3)
JCSD – 40
UPAD – 6 (2)
ASOS – 4
JFHQ-IN – (4 )

( ) = non-participant / support role

Additional:
Role Players – (50)

IPR #1 10SEP20 → **CDC** 06-08OCT20 CAIN/MUTC → IPR #2 1NOV20 → IPR #3 4DEC20 → **IPC** 2-3MAR21 MS Teams → **MPC** 16-17MAR21 MUTC → **FPC** 11-12MAY21 MUTC → IPR #4 21JUN21 → IPR #5 19JUL21 → **Execution** 13-15AUG21 MUTC

# Homeland Defender Key Events Timeline

1-12 AUG 21 Local media reports increased cyber activity to local municipalities

0330 13 AUG 21 – 4.3 MAG Earthquake

13 AUG 21 – HAZMAT call out initiates Rail Yard and Hospital Scenarios (Lanes 1 and 3)

13 AUG 21 – Second Earthquake Occurs causing multiple structure collapses (Lanes 5 and 6)

13 AUG 21 – IC Requests additional resources from JC-EMA (Lanes 2)

13 AUG 21 – State EOC assigns INNG Forces to IC

13 AUG 21 – NGRF arrives to secure govt. center (Lane 12)

14 AUG 21 – Search and Extraction of structure collapses (Lanes 5 and 6)

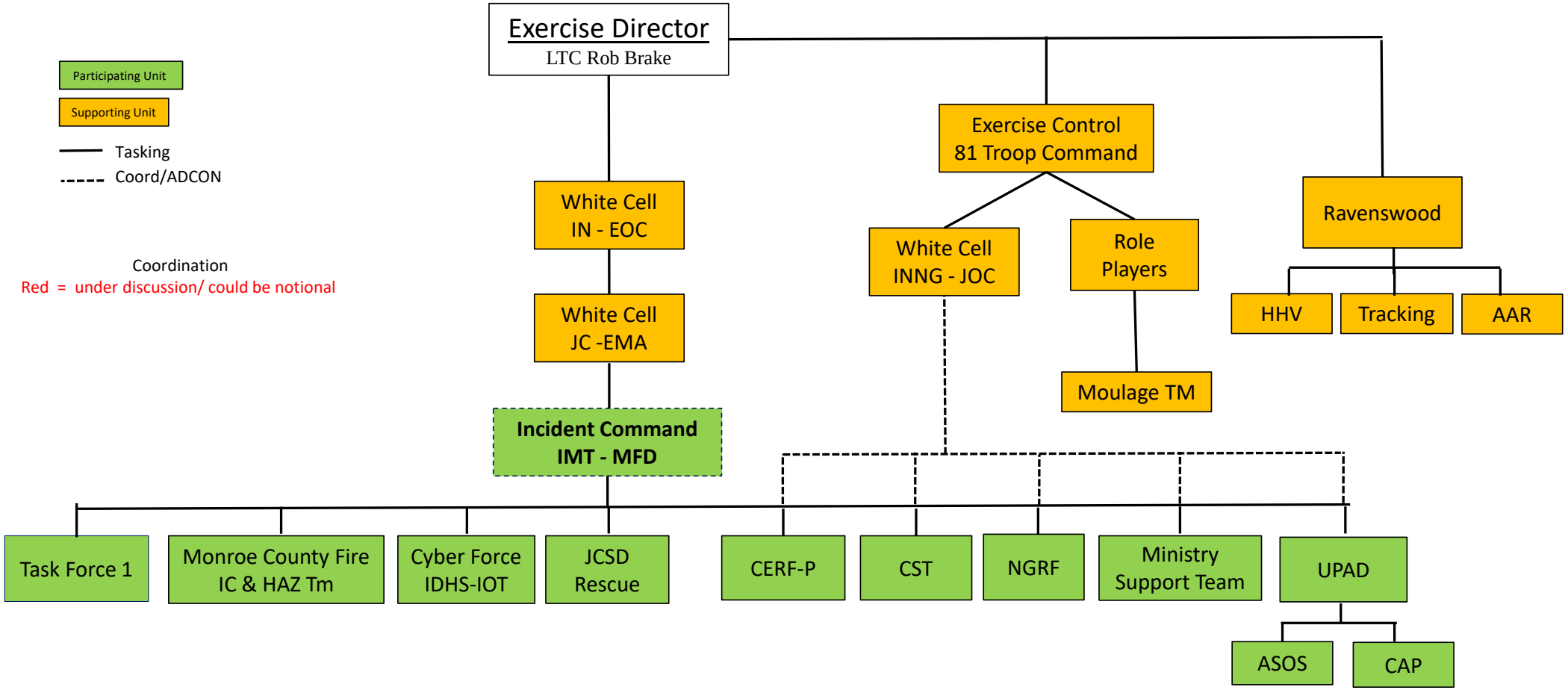
14 AUG 21 – Cyber ransom attack at water treatment facility (Lane 9)

14 AUG 21 – Increase civil unrest at govt. center (Lane 13)

14 AUG 21 – Wide area search for lost personnel (Lane 8)

INDIANA NATIONAL GUARD

# Task ORG



# Indiana's Cyber Readiness Advancing Rapidly

Friday, October 1, 2021

If you think about it, protecting a school, hospital, or a city's water supply from a cyberattack is a lot like a football coach drawing up a game plan for playing against the #1 team in the country – every day.

There's game film, playbooks and you always have to account for how you're going to stop the other team's best player from scoring; all the while trying to figure out what else the coach might have up his sleeve. And there's no halftime show to try and adjust to stage a comeback.

That's the challenge facing the State of Indiana in its efforts to continue rapidly moving forward in its mission to further strengthen its cybersecurity resiliency and response.

The progress that's been achieved comes as the State of Indiana and the Indiana National Guard recently hosted two cyber exercises in a partnership with several federal agencies, health care providers, and technology companies, water utility service providers, state, and local government officials, as well as state and federal emergency and law enforcement agencies.

"Conducting these exercises highlights the strength of the cybersecurity structure that exists within the state and underscores the work that's been accomplished over the past three years by

Indiana Governor Holcomb's Executive Council on Cybersecurity with our partners in the military, academic, public and private sectors," said Indiana Department of Homeland Security Executive Director Stephen Cox. "Most importantly, it represents the progress with cyber that's been achieved on behalf of all Hoosiers when we approach cybersecurity as something that is not solved by one entity alone, but by everyone at all corners of the state."

Having a playbook is especially crucial, given the fact there are not only a seemingly endless number of situations in which a cyberattack or incident can occur, but there are all kinds of circumstances and variables that can interfere with a cyber team's strategy for protecting its systems.

**When Water Runs Out…**

A water utility being attacked is not only scary to every city in America, but the reality of it also happening is real.

The Cybersecurity and Infrastructure Security Agency (CISA) has partnered with the State of Indiana and the City of Fort Wayne to exercise how state, federal, mutual aid, and local government would work together in a long-term cyberattack that eliminates the supply of water from the city, with a special emphasis on the secondary effects for the city's hospitals.

As the Cybersecurity Program Director for the State of Indiana, there's no question cybersecurity impacts every aspect of our daily lives. As we've seen with recent cyber incidents – everything from pipelines to water utilities to schools and hospitals – a cyberattack can create substantial effects and damage to our community and our critical infrastructure, disrupting our daily lives and safety.

**When Natural Disasters Hit…**

Following the completion of the tabletop exercise, a second cyber exercise as part of a full-scale functional exercise hosted by the Indiana National Guard for first responders and several military branches as well as search and rescue teams at the Muscatatuck Urban Training Center.

The grounds of the 1,000-acre facility, located in Southern Indiana, is a real city that includes a built-in physical infrastructure, a well-integrated cyber-physical environment, an electromagnetic effects system and human elements. There are more than 190 brick-and-mortar structures with roughly 1.5 million square feet under roof, 1.8 miles of subterranean tunnels, a cave complex, more than nine miles of roads, managed airspace, a 185-acre reservoir, and a cyber live-fire range.

The focus of the Indiana National Guard exercise centered on measuring how federal, state, local and private sectors respond to a devastating earthquake.

"We really need to prepare now for these acts which we've already seen here in Indiana and across the world," said Ron Pelletier, founder and chief customer officer at Pondurance, a cyber security company.  "When natural disasters hit all parts of the world, we are seeing more and

more targeted cyberattacks in those affected areas. Investing now in preventative measures is the best way to avoid situations like that from becoming worse. It comes down to planning to avoid cyber breaches but being prepared to respond."

As emergency and military teams respond to the effects of the earthquake, the Indiana National Guard also tested the additional response of its incident command leadership while the cyber experts from IU Health, Citizens Energy Group, and Pondurance made the efforts more difficult by attacking the water supply in the aftermath.

**It's Not "If" But "When"...**

Pelletier added that Pondurance hopes disaster drills, such as these two, will raise awareness among policy makers to help fund security programs and protocols. "National, state, and community security is truly at risk here, and we need to take action now to preserve it. Waiting for the dam to burst before you repair it is a terrible maintenance strategy, and that's exactly the situation we have here across power grids, water supplies, healthcare, you name it."

Having the ability to draw on the resources and expertise required at a moment's notice to keep people safe in the event of a cyber incident or attack relies on making certain that the state and its partners have a line of communications that's always open to make sure the State of Indiana provides a response that's most effective, regardless of the circumstances.

Many of those who are participated in both state exercises also serve on the Indiana Executive Council on Cybersecurity (IECC). As defined in Executive Order 17-11 from Indiana Governor Eric Holcomb, the IECC is a first-of-its-kind collaboration, whose work as an organization within state government, is responsible for guiding the state's cybersecurity policy, It is comprised of 35 Council members and 250 advisory members, all of whom are subject matter experts represent a wide range of businesses, industries and professions, including education, finance, utilities and insurance, among many others.

The State of Indiana and its partners offer best practices, guides, toolkits, and resources to allow all organizations and critical infrastructures to mitigate, but also prepare for a cyberattack. For more information about the IECC or the State of Indiana's Cyber Strategy, visit www.in.gov/cyber.

For more information about CISA's cybersecurity services and resources, visit www.cisa.gov.

# Virtual Workshop

LIVE VIRTUAL WORKSHOP

# Indiana Water and Wastewater Utility Cyber Workshop

Following a mock disaster drill that included a water utility cyberattack in the midst of a mock earthquake, the state of Indiana with its partner organizations are offering a live virtual workshop on Tuesday, Oct. 5, at 3 p.m. ET for Hoosier, Indiana, water and wastewater utilities. Attendees will learn:

- How a cyberattack could occur in your utility today.
- How to prevent and prepare for common cyberattacks.
- Cyber hygiene best practices for water and wastewater utilities.
- A case study of the Oldsmar, Florida cyberattack.
- How to best respond to cyberattack with public and private organizations.

**CEU:** 1.5

**Cost:** Free

**NOTE: This webcast has reached the registration capacity and is no longer accepting registrants. If you have previously registered for this webcast you may login using your email address.**

romeroclm@iot.in.gov

## Presented With:

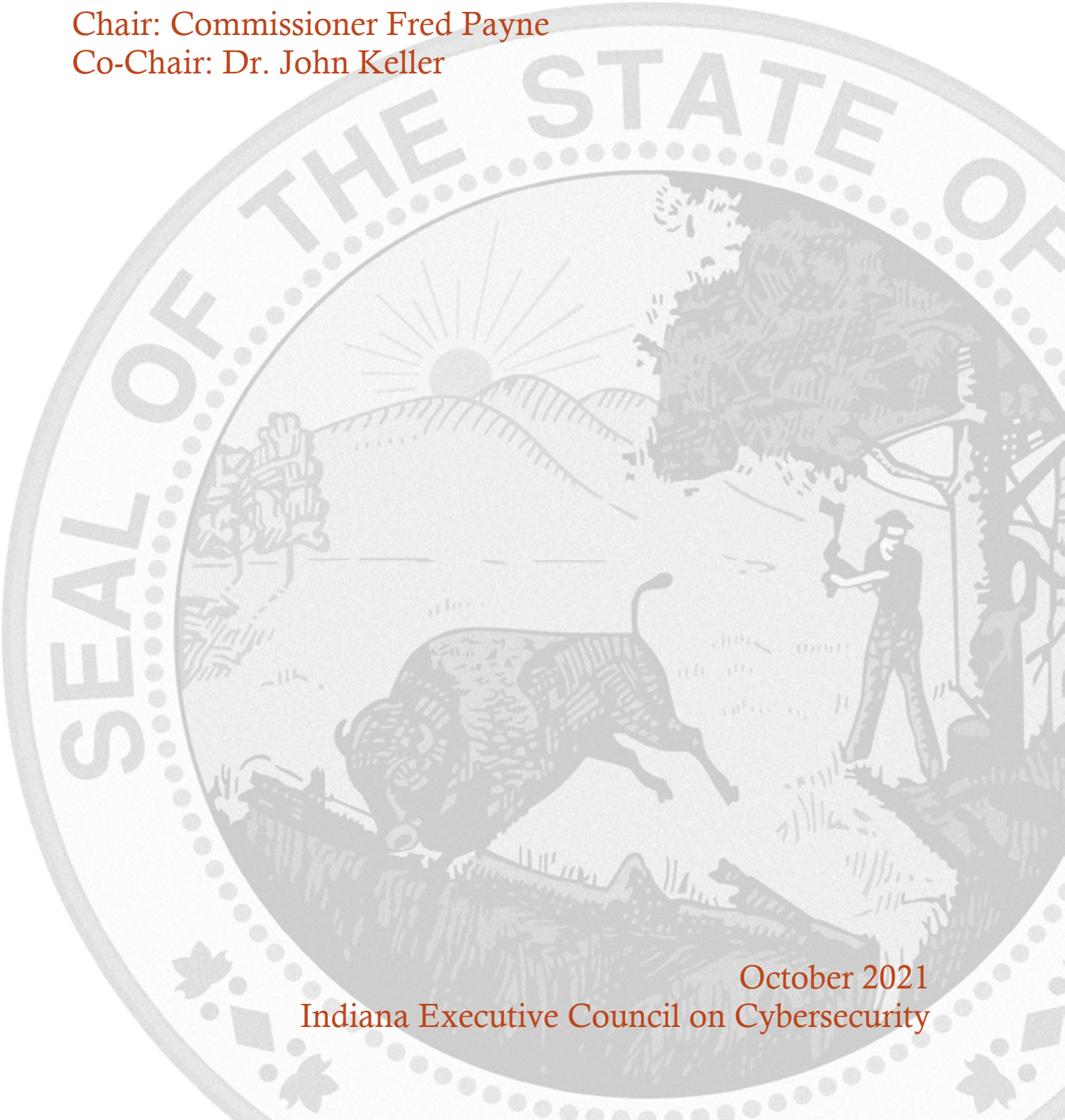

Indiana University Health

citizens energy group

# Appendix D.10
## Workforce Development Committee

# WORKFORCE DEVELOPMENT COMMITTEE STRATEGIC PLAN

Chair: Commissioner Fred Payne
Co-Chair: Dr. John Keller



October 2021
Indiana Executive Council on Cybersecurity

# Workforce Development Committee Plan

# Table of Contents

# Committee Members

## Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Akgul | Arif | Indiana State University | Assistant Professor - School of Criminology & Security Studies | Full Time |
| Bailey | George | Purdue University / cyberTAP | Assistant Director, cyberTAP / Professional Services | As Needed |
| Cloud | Matthew | Ivy Tech Community College of Indiana-Lake County Campus | Director of Cybersecurity Grants, Asst. Prof. of Data Analytics, and Dept. Chair School of IT and Criminal Justice | As Needed |
| Frank | Michael | Anderson University | Professor of Political Science | Full Time |
| Jirik | Jiri | Ivy Tech Community College | Assistant Professor - Evansville | As Needed |
| Keller | John (Dr.) | Indiana Department of Education | Chief Information Officer, IT | Co-chair |
| Knies | John | Lumen | Director Information Security | As Needed |
| Koressel | Jake | Indiana Department of Education | Computer Science Specialist | Full Time |
| Korty | Andrew | Indiana University | Chief Information Security Officer | Full Time |
| Lubbers | Teresa | Indiana Commission for Higher Education | Commissioner | As Needed |
| Mathis | Dan | Indiana Office of Technology | Compliance Manger | As Needed |
| Meadors | Joe | Gaylor Electric Inc | Vice President of Information Services | As Needed |
| Neely | Dewand | MGT Consulting | Chief Information Officer | Full Time |
| Odum | Matt | Briljent, LLC | President | As Needed |
| Payne | Fred | Indiana Department of Workforce Development | Commissioner | Chair |
| Rapp | Douglas | Cyber Leadership Alliance | President | Full Time |
| Salahieh | Rami Maximus | Ivy Tech Community College, Valparaiso, NIISSA | CSIA Program Chair, CSOC Valpo Director | Full Time |

| | | | | |
|---|---|---|---|---|
| Scarbro Kennedy | Valinda | IBM | IBM Global University Specialty Programs Manager-Medical, Legal, and HBCUs | Full Time |
| Schmelz | Pam | Ivy Tech Community College | Chair, School of Information Technology | Full Time |
| Shemroske | Ken | University of Southern Indiana | Associate Professor of Computer Information Systems | Full Time |
| Tucker | Jeff | Indiana Department of Workforce Development | Chief Information Officer | Chair Proxy |
| Rogers | Marc | Purdue University | Executive Director, Purdue Cyber Apprenticeship Program, and Clinical Professor | Full Time |
| Vespa | Tony | Vespa Group, LLC | Owner | As Needed |
| Downes | LeighAnne | Indiana Department of Workforce Development | Technology Liaison Sr | As Needed |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan.*

For more information, visit www.in.gov/cybersecurity.

# Executive Summary

# Executive Summary

- **Research Conducted**
  - Searched for:
    - Review of previous committee deliverables for updates and re-use.
    - Validate 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
  - It is difficult to understand all the training opportunities available to Indiana's labor force and talent pipeline
  - 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 widely adopted.
  - 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 up to date enough to satisfy all our committee goals.

- **Committee Deliverables**
  - Enhance CyberseekIN.org Data Tool
  - Enhance Cybersecurity Talent Pipeline and Job Openings Dashboard
  - Update K-12 Cybersecurity Content
  - Promote cybersecurity training across the K-12 sector to protect the educational process
  - Update the CHE Cyber Program Data Tool and Report

# Research

# Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity**?
   a. Inventoried cyber related course offerings available within Indiana's higher education network so we have a better understanding our education pipeline.

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 continues to be 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 National Institute of Standards and Technology (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 is now widely adopted by other states and tools are being developed to facilitate the implementation of the framework (e.g., a job description writing tool).
   b. Purdue's Cyber Apprenticeship Program, along with Indiana's Office of Work-Based Learning and Apprenticeships, offer an exciting way to connect interested talent with motivated employers.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc.**
   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 initial 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. Offering free cyber courseware online to students to promote awareness and interest of the cyber industry.

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.
    b. Ability to see current and future demand for all cybersecurity jobs.
    c. Ability to understand the skills associated with all jobs that make up the demand.
    d. Ability to see all students in the pipeline that are in programs that provide them the needed skills to fill that demand.
    e. 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: Enhance CyberseekIN.org Data Tool

# Deliverable: Enhance CyberseekIN.org Data Tool

## *General Information*

1. **What is the deliverable?**
   a. Enhance CyberseekIN.org Data Tool

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?**
   ☐ 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. Continuously updating and adding new functionality to a “go to” site dedicated to Cybersecurity occupations/training for the State of Indiana helps to strengthen the focus on a growing industry sector for talent and employers.

6. **What metric or measurement will be used to define success?**
   a. Data analytics to monitor usage and length of site visit including page access as well as other “clicks” within the site to determine user movement.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. Job Seekers and Employers as well as other workforce development and training entities

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Some cybersecurity occupations/job postings/training options are visible in Indiana Career Connect and Indiana Career Ready sites operated by the Department of Workforce Development.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. No Response

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 is working with Burning Glass Technologies, Purdue University's PCAP program as well as a group of training providers and employers.

12. **Who should be main lead of this deliverable?**
    a. Department of Workforce Development – IT Department

13. **What are the expected challenges to completing this deliverable?**
    a. Because cybersecurity is an emerging occupation group, some national data links such as CIP & SOC codes as well as ONET data have not yet categorized occupations in this industry with their own set of identification codes – many occupations (under cybersecurity) are sharing industry codes with other industry sectors employing similar occupations.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Integrate CyberseekIN with CHE's Credential Engine | DWD | 0 | June 2022 | Need to understand CE roadmap and timelines |
| Refresh Training providers in Cyberseek | DWD | 0 | October 2022 | Initial launch was a one-time feed of training providers |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1 | 1 | Project Management | TBD | TBD | Staff and outside vendor to complete all edits |

**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 |
|---|---|---|---|---|---|---|
| Burning Glass Technologies | Hosting of site | $140,000 – development and site hosting costs | TBD | TBD | TBD | Site is part of DWD's 3 year contract with BGT |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. One stop shop for Cybersecurity job seekers, employers, and training provider information

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

a. The site will educate Hoosiers on the cyber security industry and what occupations are available relative to what education is needed to be successful.

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

a. Not building an insource of talent to full fill the Indiana employers growing need for cybersecurity specific talent. Indiana is exposed to employers seeking talent outside of Indiana as well as locating any business growth opportunities to states/countries that can meet their growing need.

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

a. Data analytics can be added to the site to monitor traffic usage and length of stay

**21. 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. Burning Glass Technologies built a national cyberseek.org site that is currently operational and linkable from the Indiana site. This site provides cybersecurity information nationally.

**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?**

☐No ☒ Yes

## Other Implementation Factors

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

a. Budget: not having the funding to continue to host and enhance the site.
b. Resources: not having participation of training providers, employers and job seekers could negatively impact the validity of the site.

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

☒No ☐ Yes

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

a. Currently, DWD is committed to providing data and resources as needed to continue the site data and hosting. Finding and securing funding is always a necessity.

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

a. This deliverable is already built and launched.

**27. Can this deliverable be used by other sectors?**

☒No ☐ Yes

a. This site is specifically designed to enhance Indiana's presence in cybersecurity industry sector. Other business sectors do have access to this site and can use this site to fulfill their business needs for cybersecurity.

.

## Communications

---

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

a. Site is fully operational and has been launched. There have been some communications released from DWD's Marketing and Communications group. Other opportunities to bring attention to the site is needed. DWD is open to participating with interested groups to further bring awareness to the tool.

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

☐No ☒ Yes

a. The tool currently links to the Indiana's cybersecurity website.

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

a. The site was featured as part of the Indiana Chamber of Commerce cybersecurity forum held this past July 2021. So continued marketing such as this will need to be done through partners and associations.

## *Evaluation Methodology*

**Objective 1:** Indiana DWD will add Credential Engine certifications data to CyberseekIN.org (training providers) by June 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

**Objective 2:** Indiana DWD continue Data enhancements to CyberSeekIN.org including continual updates to training providers, Apprenticeship Data/Opportunities, and Promote opportunities, training, events surrounding cybersecurity in Indiana by October 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: Enhance Cybersecurity Talent Pipeline and Job Openings Dashboard

# Deliverable: Enhance Cybersecurity Talent Pipeline and Job Openings Dashboard

## *General Information*

1. **What is the deliverable?**
   a. Cybersecurity Talent Pipeline and Job Openings Dashboard

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?**
   ☐ 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. Create a dashboard measuring Indiana's job demand, talent pipeline, apprenticeships and training opportunities

6. **What metric or measurement will be used to define success?**
   a. Create a data collection tool to use for informational purpose to power the dashboard with the most up-to-date demand, pipeline as well as apprenticeships/training opportunities. Final measurement would be a published dashboard.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Job Seekers, Training Providers, employers s

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. Some cybersecurity occupations/job postings/training options are visible in Indiana Career Connect and Indiana Career Ready sites operated by the Department of Workforce Development.

## 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. DWD would need to be involved based on the multiple avenues we currently have for data collection. Would also use DOE and Apprenticeship

12. **Who should be main lead of this deliverable?**
    a. Department of Workforce Development – IT Department

13. **What are the expected challenges to completing this deliverable**?
    a. Because cybersecurity is an emerging occupation important data codes may bridge across multiple industries.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Analysis of current dashboard data sets and metrics | DWD | 10 | 11/1/2021 | |
| Analysis of potential data sets and how they could be incorporated into existing dashboards | DWD/BG | 0 | 12/1/2021 | |
| Implement changes to dashboard with cyberseek | BG | 0 | 1/31/2022 | May require contract amendment |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1 | 1 | Research and Project Mgt | TBD | TBD | Staff and identified other resources |

**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 |
|---|---|---|---|---|---|---|
| TBD | | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Help Indiana keep a pulse on a growing industry sector and show Hoosiers a growth pattern in cybersecurity.

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

a. The site will educate Hoosiers on what cybersecurity opportunities are available and what training needs exist to support the roles.

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

a. Not building an insource of talent to fulfill the Indiana employers growing need for cybersecurity specific talent. Indiana is exposed to employers seeking talent outside of Indiana as well as locating any business growth opportunities to states/countries that can meet their growing need.

**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 defined as a completed dashboard that integrates real time data for cybersecurity employment and training provider information

**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 at this time

**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 at this time

## Other Implementation Factors

---

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

a. Budget: not having funding to follow through with development of a robust system
b. Resources: not having needed participation of training partners, employers and job seekers

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

☒No ☐ Yes

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

a. Partnerships with other agencies as well as outside companies support the data needed to power the dashboard can be researched, but creating partnerships is even more collaborative.

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

a. DWD - IT

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes,

## Communications

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

a. Unknown

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

☐No ☒ Yes

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

a. Undetermined at this time.

## *Evaluation Methodology*

**Objective 1:** Indiana Department of Workforce Develop create cybersecurity workforce dashboard metrics – measuring Indiana's job demand, talent pipeline, apprenticeships, and training opportunities by January 2022.

*Type:* ☒ Output ☐ Outcome

☒ 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: Update K-12 Cybersecurity Content

# Deliverable: Update K-12 Cybersecurity Content

## *General Information*

1. **What is the deliverable?**
   a. Develop and promote high school CTE programs of study.
   b. Increase the number of K-12 staff equipped to teach cybersecurity related courses and courses incorporation cybersecurity related content.

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?**
   ☐ 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. In conjunction with the Governor's Workforce Cabinet and the IDOE will support the development of high school Career and Technical Education programs of study in Cybersecurity and support efforts to increase awareness of such programs with students, families and parents. The IDOE's support will include developing resources for instructors to help them deliver cybersecurity content to students in the courses and programs on this topic. IDOE will develop and curate professional development resources on cybersecurity across the K-12 continuum.

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. Number of individuals receiving industry credentials or certificates from completing cybersecurity classes (post-graduation)
   e. Number of individuals participating in educational and experiential programs

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

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 cybersecurity 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. State or Federal STEM/Computer science programming and funding opportunities.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Governor's Workforce Cabinet
    b. Professional development providers
    c. Commission for Higher Education

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. IDOE along with those who provide content/training for the proposed K-12 computer science offerings across the state.
    b. Governor's Workforce Cabinet (GWC)
    c. Commission for Higher Education

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

a. IDOE/GWC

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

a. Ensuring that consistent (and correct) content is included in all 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. Statewide implementation

## *Implementation Plan*

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

☐ One-time deliverable
☒ Ongoing/sustained effort

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Include cybersecurity topics as part of ongoing computer science professional development for K-12 teachers. | IDOE | 25 | Fall 2023 | This program of study is available for adoption by all Indiana High Schools. |
| Promote the development of a Cybersecurity program of study | GWC | 100 | Spring 2021 | This content will be available through the Learning Lab (Digital platform sponsored by IDOE to distribute Professional Development) and on the IDOE web site. |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| None | | | | | |

**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 |
|---|---|---|---|---|---|---|
| Expert Consultation | Guidance and project management to develop Cybersecurity standards for K-12 | TBD | TBD | State/Federal | Grants | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Opportunities for high school students to earn workforce relevant cybersecurity skills and credentials with support from high quality instructors.
b. Opportunities for teachers to improve their instructional skills in the area of cybersecurity and computer science.

**18. How will this deliverable reduce the cybersecurity risk or impact? What are 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.
   ii. Increasing the pool of available job seekers with relevant cybersecurity credentials.

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

a. Lack of opportunities for Indiana students to receive relevant preparation for the workforce. May impact the competitive edge for Indiana if we must always import cybersecurity professionals to meet the growing demand.

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

a. Number of Indiana high school students earning industry recognized cybersecurity credentials.
b. Number of teachers available to meet demand for cybersecurity related courses.

**21. 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

**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?**

☐No ☒Yes

## Other Implementation Factors

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

a. Any results with direct impact to the economy are years away.

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

☒No ☐Yes

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

a. Ongoing investment in this programming and ensuring its availability across schools and geographies.

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

a. This deliverable is consistent with interagency plans being developed by the Governor's Workforce Cabinet, Indiana Department of Education, and Commission for Higher Education.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. Creating more potential job candidates would help any sector needing cybersecurity professionals and expertise.

## Communications

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

a. Indiana K-12 schools

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

☐No ☒ Yes

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

None at the moment.

## *Evaluation Methodology*

**Objective 1:** Governor's Workforce Cabinet with support from IDOE will develop and promote a high school CTE Program of Study in Cybersecurity by June 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

**Objective 2:** Indiana Department of Education will develop a menu of cybersecurity-related professional development and resources, including K-12 computer science offerings, by June 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

**Objective 3:** Indiana Department of Education and Cybersecurity Program Director will edit and distribute the Cybersecurity for Education Toolkit 2.0 by February 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: Promote Cybersecurity Training Across the K-12 Sector to Protect the Educational Process

# Deliverable: Promote cybersecurity training across the K-12 sector to protect the educational process

## *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?**
   ☐ Completed ☒ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

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. 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?**
   ☐ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

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?**

☐ One-time deliverable
☒ 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 2023 | 16-17 school year there were 167 Indiana Schools Certified (https://d1e2bohyu2u2w9.cloudfront.net/education/sites/default/files/certified_schools_16_17_final.pdf) |
| Develop K-12 appropriate emphasis for Cybersecurity Month in October | IDOE | 0 | October 2024 | 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 2024 | 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 | 2023 | This is a three-phase program. Phase one includes 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 2024 | |
| Promote the development of a Cybersecurity Graduation Pathway | SBOE | 0 | 2024 | 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 2024 | 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 2024 | 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 | IDOE | 0 | September 2024 | This is a big lift but would really help to lay the foundation for moving from |

| | | | | |
|---|---|---|---|---|
| for cybersecurity across the K-12 curriculum | | | | 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 2023 | 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 | 2024 | This is part of the IN CyberPath project with Purdue and IU |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| 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?**

| 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?**

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 are the estimated costs associated with that risk reduction?**

a. This would reduce the cybersecurity risk or impact in three 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?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. 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?**

☐No ☒ Yes

a. 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?**

☐No ☒ Yes

a. 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)?**

☐No ☒ Yes

a. If formal steps were taken in this area, it should 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:** The joint Cybersecurity Task Force ensure more than 75,000 staff and students are delivered training and phishing support through the KnowBe4 platform by December 2024.

*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 joint Cybersecurity Task Force will raise awareness of schools to digital threats to the educational process by raising awareness through monthly newsletters, and by working with partners to provide professional development for school IT staff by December 2024.

*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:** DOE will work to encourage all schools to appoint one staff member to monitor information releases from the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Indiana Information Sharing and Analysis Center (IN-ISAC) 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

**Objective 4:** Create a DOE Moodle Community to share school cybersecurity information with public, religious, and private schools as well as provide opportunities for secure collaboration and sharing of best practices by December 2021.

*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: Update the CHE Cyber Program Data Tool and Report

# Deliverable: Update the CHE Cyber Program Data Tool and Report

## *General Information*

**1. What is the deliverable?**

a. Updated 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.

**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?**

☐ 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. Expands the capability of the IECC to fully understand the supply of qualified graduates and their credentials/degrees to make better informed policy decisions.

6. **What metric or measurement will be used to define success?**
   a. If success refers to the deliverable – then timely delivery of report by 3/31/22. Resulting policy decisions.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Most directly the IECC will benefit to make informed policy decisions.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. None directly we are aware of. Of note: https://www.nist.gov/itl/applied-cybersecurity/nice

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None this time but this could change in the future.

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. Institutions of higher education in Indiana.

12. **Who should be main lead of this deliverable?**
    a. Commission for Higher Education

13. **What are the expected challenges to completing this deliverable?**
    a. Availability of time and resources.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| CHE team planning meetings, prep and data querying for current program codes | Rajinder Heir, Academic Affairs, Policy & Research | 100 | | Initial inquiries and tasks started in Jul & Aug. |
| Notification to Academic Officers at Institutions to report Cybersecurity related students/degrees/programs | CHE Academic Affairs | | 9/30/21 | |
| Begin analysis and synthesis of data from Institutions on Students/Degrees/Programs and develop report on Findings | CHE Policy & Research, Academic Affairs | | 11/29/21 | |
| Distribute final report | CHE | | 3/31/22 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

a. CHE staff time required

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| .15 | | Data Analysis and more | | | 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. Other staff will be involved – coordination, academic affairs team, possibly graphic designer. |

**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 |
|---|---|---|---|---|---|---|
| Office productivity software, graphics software. | | No Response | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

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 are the estimated costs associated with that risk reduction?**

a. The state's capacity to insource and grow cybersecurity expertise will mean less financial risk as we will be better able to recruit graduates from Indiana colleges to work for Indiana organizations.

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

a. If we don't understand the supply-side of the equation, we may have to outsource cybersecurity jobs/contracts to other states and/or 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 public and private sectors 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?**

- Major-level data on cybersecurity-related degrees.
- Minor-level data would also be helpful to understanding the supply.
- Data to understand the extent to which programs have cybersecurity content.

**21. 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

**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?**

☐No ☒ Yes

## Other Implementation Factors

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

a. If additional deliverables/requirements 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.

b. We count on the institutions to deliver the data we request in a timely fashion and have no reason to expect this will not happen. However, it is an implementation risk factor.

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

☐No ☒ Yes

a. We may want to require Institutions to report more granular data than degree-level. This could be codified, but likely will require additional conversations.

**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. The CHEDSS system is current under a re-write effort.

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

a. This deliverable has been discussed internally at CHE at least through the collection of the data. Staff at CHE will now contact Academic Officers at Indiana institutions to collect survey data for the second iteration of the report.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. Less so as it stands, however expanding the collection of this major-level data to non-cybersecurity fields can potentially generate uses for additional domains.

## 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)?**

☐No ☒ Yes

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

a. None at this time.

## *Evaluation Methodology*

**Objective 1:** Commission for Higher Education will re-launch survey/tools to capture and collect program course curriculum to help the IECC understand and inventory which higher ed schools are providing cybersecurity related training programs by December 2021.

*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:** Commission for Higher Education will update the Cyber Program Data Tool and Report by March 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

# 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.

- CHE Cyber Program Data Report 1.0
- Cybersecurity for Education Toolkit 1.0

# CHE Cyber Program Data Report 1.0

INDIANA COMMISSION for HIGHER EDUCATION

# Report to the Indiana Executive Council on Cybersecurity

Cybersecurity is at the top of mind for Indiana employers, as well as the state's higher education institutions to ensure the state is producing the necessary talent to meet employer demand and provide a safe and secure digital landscape for all Hoosiers.

While the Indiana Commission for Higher Education had some data on Cybersecurity and related degrees currently being offered in the state, a deeper dive was required to fully understand the options available to students.

Often, Cybersecurity coursework and degree options are "hidden" within other computer and information science programs. With that in mind, the Indiana Executive Council on Cybersecurity's Workforce Development subcommittee pursued a closer look at the richest sources of programmatic data – Indiana's public institutions.

The Commission recently surveyed these institutions to assess how they are prioritizing Cybersecurity content in current and planned computer science and technology curricula. The results of those surveys are summarized in this report.

Several themes emerged in the survey's results about how the state's institutions offer Cybersecurity curricula. Enrollment and graduate numbers, for example, have remained steady or increased over time. And while institutions offer a wide array of education related to technology and computer and information science, a range of Cybersecurity content is embedded in current program offerings.

## Enrollment and graduate number highlights

While overall college enrollment has experienced a small decline in recent years (from 65 percent in 2017 to 63 percent in 2019), there has been a steady increase in the number of students enrolling in Information Technology and Cybersecurity-related degrees in Indiana's public and private colleges and universities.

There were over 56,000 enrollments in Information Technology and Cybersecurity-related programs across the state between 2015 and 2019, with Indiana's public colleges representing almost 50,000 of those enrollments. Including the state's private colleges, there were over 7,000 students enrolled in Information Technology and Cybersecurity-related programs between 2015 and 2019 at private, non-profit colleges; and more than 200 were enrolled at private for-profit institutions in the same time period.

Between 2015 and 2019, there were more than 10,600 degrees conferred in the Information Technology and Cybersecurity sectors for all institutions throughout the state. Again, the public institutions provide the majority of those degrees, at just over 9,000. Private, non-profit colleges (1,600 degrees) and private, for-profit colleges (44 degrees) add to the total.

While the majority of conferred degrees in these sectors are represented by Indiana's public colleges, some out of state students come to Indiana specifically seeking these degrees. The state's challenge is retaining those students who come from outside Indiana and encouraging them to stay after graduation.

Indiana's opportunities for going forward and expanding upon these sectors include paying for what we value: including certificates in growing and high-demand areas, such as IT and Business Services, through the state's Workforce Ready Grant.

Additionally, as Central Indiana in particular has become a technology hub in the Midwest, connecting students to local employers who can offer work-based experience and internships will encourage more of these students to make connections and develop roots in the state. This, in turn, provides more opportunity for students to stay in the state after graduation – particularly those that move to Indiana to pursue higher education.

IT and Cybersecurity program enrollment and graduate highlights:

- Purdue West Lafayette anticipates about 150 students graduating with the Computer & Information Technology Degree (with a Cybersecurity major) in 2021 with small numbers of students who switched majors graduating in 2018 and 2019
- Purdue Northwest has 208 students enrolled in the Cybersecurity major as of Fall 2019
- Indiana State University expects to graduate about 20 students from the Cybercriminology and Security Studies program, starting in 2022
- Ball State has a master's of science minor in Computer Security with 25 students enrolled in the spring 2019

## Cybersecurity curriculum

A range of Cybersecurity content is included in the current Computer Science curricula for the bachelors of science and bachelors of arts degrees at Indiana's public institutions.

Cybersecurity coursework content ranges from as little as under **6 percent** (Indiana University South Bend) to as much as **over a quarter** of the curriculum (Indiana University Purdue University Indianapolis-Purdue).

The average Computer Science curriculum contains over 12 percent Cybersecurity content and the median Computer Science curriculum contains 10 percent Cybersecurity content.

The state's institutions are also creating new cybersecurity coursework, including a Cybersecurity Minor and Cybercriminology and Security Studies Program at Indiana State University. The University of Southern Indiana created a Cybersecurity Certificate program in the fall of 2019.

**By institution: A closer look**

The **Purdue Northwest** bachelors of science Computer Information Technology degree program has been recognized by the NSA as a Center of Excellence in Cybersecurity. Purdue Northwest was designated in 2014 and re-designated in 2019 by the U.S. Department of Homeland Security and the National Security Agency as a National Center of Academic Excellence in Cyber Defense Education.

At **Purdue West Lafayette**, the Cybersecurity major has grown significantly between 2016 and 2018. While students began joining the major in the years prior, there were 171 students in 2017 and 232 in 2018. The major represents about 40 percent of the B.S. degree in Computer and Information Technology students in 2018. Purdue West Lafayette has been designated as a Center of Academic Excellence in Research by the U.S. DHS and NSA.

**Indiana University and its regional campuses** offer cybersecurity courses and degrees ranging from certificates to doctorate-level degree programs. Indiana University has been designated as a Center of Excellence in Cyber Defense and Center of Excellence in Research by DHS and NSA.

At **Ball State University,** the Computer Science degree has a significant focus on cybersecurity, representing 18 percent of the degree coursework. The spring 2019 enrollment in Computer Science was 388 students. The school also offers a master's Computer Security minor (25 students were enrolled in spring 2019).

**Indiana State University**'s Information Technology Program has a cybersecurity component which makes up approximately 10 percent of the program's coursework. The new Cybercriminology and Security Studies Program has grown from 27 students enrolled in fall 2018 to 66 students enrolled in fall 2019.

The **University of Southern Indiana** developed a Cybersecurity certificate program that began in fall 2019. Some classwork in this program is currently a requirement for the Computer Information Science majors.

The **Vincennes University** College of Technology offers a Computer Networking Fundamentals Certificate, which is a one- to two-year certificate with about half of the total credit hours devoted to Cybersecurity content. The university also offers an associate degree for a Computer Network + Security Specialist, with 41% of the total coursework dedicated to cybersecurity.

At **Ivy Tech Community College,** there are options to pursue a certificate, technical certificate and associate degree in Cybersecurity and Information Assurance; the program is focused entirely on cybersecurity. Ivy Tech Community College has been designated by the U.S. DHS and NSA as a Center of Academic Excellent in Information Assurance – 2 Year Education.

## Conclusion

As Hoosiers' lives are increasingly connected to digital devices and the Internet of Things continues to gain global traction, the potential threats to Indiana's security also increases. Meeting Indiana's need for high-quality Cybersecurity education and training options must remain a priority for the state's higher education institutions and the state as a whole.

Preparing for the future of Cybersecurity issues in Indiana begins with ensuring there is a sufficient statewide pipeline of talented professionals ready and able to take on the challenge of keeping the Hoosiers safe and secure for years to come.

This is a career path that is in high demand, with more than 2,300 open Cybersecurity positions in Indiana currently, according to the Indiana Cybersecurity Hub. While our public institutions are emphasizing and growing the educational tracks and curricula to support Cybersecurity and related fields, more prominence must be paid to these career paths in order to fill these positions and prepare for anticipated growth in this crucial field.

# Cybersecurity for Education Toolkit 1.0

# CYBERSECURITY FOR EDUCATION TOOLKIT

Cybersafe Tips & Resources for Indiana's School Communities

# Cybersecurity for Education Toolkit

*Developed by the Indiana Executive Council on Cybersecurity*
*August 2020*

## Table of Contents

# HOW TO USE THIS TOOLKIT

Regardless of the important role you play in educating our children and young adults, this *Cybersecurity for Education Toolkit* is designed for you.

Whether you are a superintendent, administrator, teacher, or staff member, we encourage you to use these materials – and share them with your colleagues, students and others in your school community – as a turnkey resource; saving you precious time as you focus on the rapidly increasing challenges that are taking place in education as the school year gets underway.

In fact, we have created the toolkit in a Word Document format that will enable you to cut and paste, copy and/or repurpose all the articles, images, and social media posts in the *Toolkit* as needed.

In addition to these materials, we invite you to visit our Cybersecurity Hub Page located on the website of the State of Indiana at www.in.gov/cyber. There, you will find even more resources – updated frequently -- that will help you with everything from tips on maintaining good cyber hygiene to the steps you should take if you are the victim of a cybercrime.

Developed by the members of the Indiana Executive Council on Cybersecurity (IECC) including the Indiana Department of Education, our Cyber Hub feature sections for Educators (https://www.in.gov/cybersecurity/3827.htm), Teachers (https://www.in.gov/cybersecurity/3836.htm), Students (https://www.in.gov/cybersecurity/3830.htm), and much more!

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

September 2020

Dear School Community Member:

With the school year underway – inside classrooms and virtually – across Indiana, **cybersecurity** is one of the keys to achieving a higher level of education, safely and securely.

To help our school communities continue to be strong and protected while staying connected, the Indiana Executive Council on Cybersecurity (IECC) along with the Indiana Department of Education has developed this *Cybersecurity for Education Toolkit* for everyone, including:

- Superintendents and School Board Members
- Teachers, staff, and administrators
- Students of all ages and their families
- Every person who lives in our school communities

Our toolkit is designed to be easy-to-understand resource, complete with tips and helpful information to make sure you are cybersafe and practicing good habits that will help:

- Students protect their identity and schoolwork
- Teachers and staff manage their lesson plans and keep safe their student's data, including their grades and assignments
- Administrators protect their students and keep secure their facilities
- Members of the public can engage and communicate with schools and educators

Most importantly, this guide is intended to provide you with resources to get started and more information about online learning. You are also welcome to visit the website for the Indiana Department of Education at https://www.doe.in.gov or check out their *Digital Education Toolkit*. Additionally, there are other materials in the toolkit, including content for use on social media platforms, including Twitter, Facebook, and LinkedIn. Also, we have included a selection of blogs and brief bylined articles – from a variety of trusted sources – that the IECC encourages you to share with teachers, families, and your communities.

You are also welcome to visit Indiana's Cybersecurity Hub Page (www.in.gov/cyber) for an even more resources you'll find valuable -- inside and outside of the classroom. We look forward to your input on this toolkit as we seek to improve it over the coming months and that it will serve as a helpful guide for being safe when you and our children are online.

Sincerely,

Chetrice L. Mosley-Romero
Cybersecurity Program Director
State of Indiana
MosleyCLM@iot.in.gov

Dr. John Keller, CTO, Indiana Department of Education
Workforce Development Committee Co-Chair
Indiana Executive Council on Cybersecurity
jkeller@doe.in.gov

# PROTECT YOUR SCHOOL

## *Article 1:*
## *The Importance of Cybersecurity to Your School's Infrastructure*

As a school superintendent, together with your administrators, you are tasked with the day-to-day responsibility of protecting your schools, students, teachers, and staff on behalf of the community.

And, in collaboration with the members of your school corporation's board, you are always working proactively to adopt policies to help ensure that your students learn and are provided with an education in an environment that is safe and secure and that's especially true as it involves cybersecurity.

Following on the experiences thrust on schools at the start of the Pandemic, there are a great deal of resources out there to help guide your school's approach to being cyber safe for everything from your infrastructure to the security of your student's personal data, as well as your curriculum and the lesson plans created by your teachers and staff.

According to the National Cyber Security Alliance (www.staysafeonline.info), it is important to routinely evaluate, update, and implement your cybersecurity plans. This includes protecting your schools by following these 10 tips for anyone who relies upon computers in your school district:

- Use anti-virus software.
- Don't open e-mails or attachments from unknown sources. Be suspicious of any email attachments from unknown sources. Also, be suspicious of any email attachments that are unexpected, even if they come from a known source.
- Protect your computer from Internet intruders.
- Regularly download security updates and patches for operating systems and other software.
- Always use hard-to-guess passwords. Mix upper case, lower case, numbers, and other characters not easily found in the dictionary. Make sure your password is at least eight characters long.

- Routinely back up your computer data on disks or CDs regularly.
- Don't share access to your computer with strangers. Learn about file-sharing risks.
- Disconnect from the Internet when not in use.
- Check your security on a regular basis.
- Make sure all your teachers, staff and administrative team members know what to do if a computer or system is believed to be infected or corrupted.

It's also a good idea to raise awareness with your students on why being cybersafe is important and use social media to disseminate information and encourage students, faculty, and staff to learn more about staying safe online visit www.in.gov/cyber, staysafeonline.org, and stopthinkconnect.org.

# *Article 2:*
# *Collaborate with Your School Board Members About Cybersecurity*

For school board members, adopting acceptable/responsible use policies and other important standards related to the use of technology, is at the heart of your responsibilities to the public and the larger school community.

It is important to know that cybersecurity is associated with risks that can catch even the most experienced board members off guard. Cybersecurity treats should be treated like any other kind of risk for your school district. Because of that, the same amount of detail and preparation associated with mitigating financial risks should be implemented when preparing for, conducting, and participating in school board cybersecurity training.

According to *Diligent Insights*, to begin to develop and establish cybersecurity training for your school board, there are core steps that need to be explored and addressed.

*Diligent Insights* and *K-12 Cyber Secure* highly recommends your school board members collaborate on adopting cybersafe and acceptable use policies for your school community, which include the following:

1. Note any cyber incidents that have occurred in your district the last few years
2. Identify cybersecurity risks and issues that the board and district may face
3. Determine who will be involved in the board's cybersecurity training
4. Develop a plan of action regarding cybersecurity in your school district
5. Identify how to measure the sufficiency and effectiveness of your district's cybersecurity program
6. Determine how much your IT budget is being spent on cybersecurity-related activities and risk management

For more information, visit:

- *Core Steps for Establishing Board Cybersecurity Training* https://insights.diligent.com/cybersecurity-public-education/core-steps-establishing-board-cybersecurity-training.
- *K-12 Cybersecurity: Role of the School Board* https://k12cybersecure.com/blog/k-12-cybersecurity-the-role-of-the-school-board/
- *Campus Safety Magazine* Webinar -- *Here's How an Indiana School District Used Integrated Access Control to Bolster Security* https://www.campussafetymagazine.com/webcast/heres-how-an-indiana-school-district-used-integrated-access-control-to-bolster-security/
- *Indiana Cyber Hub – Education Resources* www.in.gov/cybersecurity/3827.htm

# PROTECT YOUR TEACHERS

*PLEASE SHARE THE BELOW ARTICLES WITH YOUR TEACHERS VIA NEWSLETTERS, EMAIL, MESSAGE FROM THE SUPERINTENDENT, MESSAGE FROM THE PRINCIPAL, STAFF MEETING, ETC. THROUGHOUT THE SCHOOL YEAR.*

## *Article 1:*
## *Keeping Your Classroom Secure Online & Using Video*

For your dedicated teachers and staff, practicing good cyber hygiene is an important part of the school day and, especially so, when working from home or conducting class remotely.

There are four important steps to keep in mind:

- Beware of Phishing Scams
  - Use caution when opening emails – even those that appear to be from trusted sources or from senders who ask you to provide sensitive information – i.e. share student data or requests
- Encrypt Your Data (both for yourself and your students)
- Secure Your Devices from Physical Attacks
  - Use a VPN (Virtual Private Network) and Multi-Factor Authentication – to provide the greater measure of protection when it is necessary to work from home or out-of-school setting
- Follow Your School's Cybersecurity Protocols
  - Work with your IT staff on system updates/Acceptable Use Policies

Throughout a school district, everyone can benefit from a reminder, to be vigilant when it comes to practicing good habits while working online, including making sure to always:

- **Keep an updated machine.** Having the latest security software, web browser and operating systems is the best defense against viruses, malware, and other online threats
- **Protect ALL devices that connect to the Internet** – It's not just computers, smartphones and other web-enabled devices, it is crucial to provide cybersecurity for your school system's critical infrastructure systems, installed on servers that are separate from those used to store student data and your school corporation's financial systems.
- **Plug and Scan:** Be aware as "USB's" and other external devices can be infected by viruses and malware. Work closely with your IT staff to use your system's security software to scan them (if permissible) or follow your school's policy on removable media.
- **Back It Up:** Protect your valuable work, music, photos, and other digital information by making electronic copies of all information files and storing them safely.

With increasing frequency, as more family members of your teachers and staff work from home, it's important for them to be aware of their surroundings – especially if they are on a video call (i.e. Zoom, Microsoft Teams or WebEx), and that their student's schoolwork is out of view. It is also good to be aware of any potential distractions or conversations occurring in the background.

What's more, teachers and staff are uniquely positioned to educate their students about good cyber hygiene as part of their everyday assignments and in-class interaction.

**Be sure the apps and online tools you're recommending your students use meet the basic criteria for safety and privacy before encouraging students and families to download them.** It's important, too, to communicate with your students and their families and encourage them to do their due diligence when recommending to them that they download a new educational app, or using an online tool for learning that you've suggested or asked them to use as part of a classroom assignment or homework.

Here are basic tips students can share with their students when safeguarding their online data, including:

## *ALWAYS HAVE A STRONG PASSWORD*

- The first step is to **create complex passwords**. A strong password should be a mixture of upper and lowercase letters and include numbers and symbols, as this will make it less likely to be guessed by cybercriminals. You can use tools like a password meter, which calculate how difficult or easy it would be to guess or hack your password and aim for a high score for each password you create.

- Create **unique passwords for each online account**. For instance, the password for your personal Facebook account should be different from that of your personal email, which in turn should be different from the one you use to access the learning

portal at school. This means that if someone guesses or hacks one password, they won't be able to access all of your accounts.

- Try to **change your passwords frequently**. It is recommended to do this at least twice a year, but once every three months is even better and more secure, especially since the sheer number of online accounts accessed at school is so high.

- Creating complex and unique passwords and changing them continuously is a great memory exercise.

- But if it turns out to be too difficult, **try using a password manager** to generate and store your passwords on your device or browser. A password manager uses a special database to create and store strong passwords so you don't have to remember them. But you do have to be careful with that one master password.

- While using public computers or other public devices and networks, **never allow the public computer to remember or store your password**. This can open the door for others to sign in after you and access your online profiles and any other personal information that might have been saved.

- Finally, take advantage of **two-factor verification/authentication** when it is available. These systems typically require you to enter both your password and a special code sent to your phone or email. This type of authentication offers the best protection for those of your accounts that hold personal and sensitive information about you.

## *DON'T FALL FOR PHISHING SCAMS & HOW TO RECOGNIZE A SCAM*

- According to the United States Department of Homeland Security, phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by manipulating them into providing personal information to the attacker.

- There are several ways online phishing scams can happen. Some are through emails, SMS text messages, social media, and even fake tech support phone calls/voicemails.

- The best way to avoid these scams is to <u>not</u> take action based on the email – don't text the number back, don't answer phone calls when you don't recognize the number, and never give your personal information out via email to someone you don't recognize from your contact list. If you keep being targeted by the same number or email, block them, or talk to your cell phone provider about blocking the number from reaching your phone.

But before you can decide not to interact with phishing scams you need to be able to recognize them. Here are a few signs that should make you suspicious:

- **Unfamiliar sources.** If you've never interacted with this person or company before, be wary;
- **Odd email addresses.** Anyone can create a Gmail or Yahoo email account, but an established company will have its own email system: cocacola@yahoo.ph versus name.surname@coca-cola.com;
- **Too many recipients of the same message.** You should be the sole recipient of the email, or at least to know the other few people addressed in case you're not;
- **Direct requests for personal information or money.** Social Security numbers, bank account information or other passwords should not be shared with strangers just because they asked;
- **Text riddled with errors.** Cybercriminals send badly written messages to increase their chances — if grammar and spelling errors don't ring any alarm, someone is more likely to hand over the required personal information;
- **Too good to be true offers.** Murphy's law is not a law for nothing. If something seems unlikely, unrealistic or too good to be true, then it probably is;
- **Strange attachments.** An attachment should be necessary and related to the message. If not, or if the extension is odd (.exe instead of .docx), it's better to not open it.

## *USE ANTI-VIRUS PROTECTION*

- Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems. It includes computer viruses, ransomware, adware, spyware, scareware, worms and more. The damages made by malware vary from making your device more difficult to use by slowing down its functions, to more serious consequences, like controlling your device or stealing your data.

- One rather famous way of malware spreading throughout a school is the use of infected removable drives. As Microsoft's Windows Security noted, "many worms spread by infecting removable drives such as USB flash drives or external hard drives. The malware can be automatically installed when you connect the infected drive to your PC. Some worms can also spread by infecting PCs connected to the same network." Working directly in the cloud is a better option, as long as the cloud is in its turn protected.

- The most important thing you must do is to install antivirus software on all your devices to make sure you're protected no matter what you're using. (Your

technology department will likely have done this for you on any device provided by your school.) This will ensure you will avoid many cyberattacks by default or at least you'll get a notification on what seems suspect and needs more attention from your part. As a young adult, it might be hard not to expose many aspects of your personal information online, so protecting your online presence is crucial and worth the costs.

Visit https://www.vpnmentor.com/blog/teachers-guide-to-cybersecurity/ for a "Teacher's Guide to Cybersecurity." For additional resources, you can also visit www.in.gov/cybersecurity/3836.htm.

# *Article 2:*
# *Working Remotely — How to Be Safe, Secure, and Successful*

Between working at the office, or school, or remotely, the principles of security can become something of a moving target. For some, this creates an uncertainty with making sure that the right policies are applied. Reducing risk on at-home networks, keeping information secure during virtual meetings and having a strong password policy are some best practices that can be implemented quickly and effectively from wherever you are working.

## *REDUCING RISK ON HOME NETWORKS*

Home IT devices, such as unsecured off-site routers, modems, and other network devices are subject to many of the same threats as on-site business devices. They can be attacked from any device on the internet. Remote devices are also vulnerable to unauthorized access from neighbors and passersby.

As we continue to work, attend school, and connect with friends and family remotely, there are steps you can take to reduce the risk and improve the security of home networks.

- To help improve the security of your home network, the following is a list of questions to consider. In many instances, you can find answers and solutions online from trusted sources that are FREE and includes step-by-step instructions to help you. You can also consider working with an IT professional as an investment in your cyber safety.

Here's the list:

- Are your network devices physically secured?
- Have you changed the default manufacturer/administrative account password on your network devices (modem and router)? Many routers will come preconfigured with a password. The default password for most router models are easily accessible on the internet, making it extremely important to change the administrative passwords and not use the default.
- Do you have a unique password and two-factor authentication (2FA) enabled on your network devices (modem and router)?
- Do you have a password policy in place? Do you have a unique password and 2FA enabled on your internet service provider's web portal?
- If you use a mobile application for network management, do you have a unique password and 2FA enabled?

- Have you installed the latest updates for your network devices (i.e., modem, router, laptop/PC) or have you enabled auto-update with the device's administration page?
- Does your network device (router/modem) support Wi-Fi Protected Access Version 2 (WPA2) or Wi-Fi Protected Access Version 3 (WPA3)? WPA2 should be the minimum.
- Have you turned off/disabled Wireless Protected Setup (WPS) and Universal Plug and Play (UPnP) on your network? If enabled, these might allow attackers to connect to your devices without permission.
- Have you changed the Wi-Fi network name to something unique that doesn't provide any identifying information?
- Have you enabled firewall on your network devices?
- Have you disabled remote management? Most routers offer the option to view and modify their settings over the internet. Turn this feature off to guard against unauthorized individuals accessing and changing your router's configuration.
- Have you hardened your device by removing ports, software or services that are unused or unwanted?
- Do you run updated antivirus and malware protection on your device?

## *SECURITY DURING VIRTUAL MEETINGS*

In order to help protect you and your organization from potential threats, here are some cybersecurity tips on how to securely configure your virtual meetings, whether they be for work or your classroom experience.

### *Sharing of Your Information Assets During Virtual Meetings*

- Avoid adding your meeting to any public calendars or posting it on social media
- Require participants to enter an access code
- Avoid reusing access codes or meeting pins
- Distribute the meeting link and access code directly to the intended participants
- Remind invited guests not to share the access code
- Before sharing your screen, close unused windows to ensure you do not share sensitive or confidential information
- Use a privacy shield or cover over your webcam when it is not in use

### *Managing Your Information Assets and Password Policy*

- Use your organization's provided services and devices
- Do not record the meeting unless it is necessary and be aware that others may be able to record the meeting
- Disable the "Anyone Can Share" feature to prevent unauthorized screen sharing
- Muting users on entry can prevent potential disruptions
- Prevent users from sharing video by default; allow video sharing only when necessary

- Validate the participant list against invited attendees, or have participants identify themselves as they join the meeting
- Do not trust the safety of links shared in meeting chats
- Schedule "Unlisted" meetings and hide specific details, such as its host, topic, and starting time
- Do not allow attendees to "Join Before Host"
- Set up each meeting to require all attendees to enter a password
- Create a unique password comprised of upper, lower case, numbers, and special characters for each meeting
- Exclude the meeting password from attendee email invitations. Provide the password to attendees via a separate email or by phone
- On reoccurring meetings, always check to ensure one-time attendees are not included in subsequent meetings or meeting chat threads
- Do not list personal information, such as location, phone number, or date of birth on your Skype profile

Remember, just like you protect your physical assets (shed, kayak, or bike) with a padlock, you need to be sure and protect the connectivity of your devices to protect your personal information!

Taking a proactive approach to following safe cybersecurity practices will help you with addressing key topics, such as understanding the importance of terms, such as "end points" and the prevalence of ransomware attacks – issues and topics that are critical and have become more evident during this new world of COVID-19 with more staff working remotely.

Have you identified more risk than you initially realized? More information and mitigation techniques can be found at Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA).

# PROTECT YOUR FAMILIES

There is no greater responsibility for schools than providing students with a safe and secure learning environment.

At the same time, as part of the new normal, there is never been a greater opportunity to capitalize on the opportunity to educate children and young adults about the importance of digital citizenship and safely communicating online; lessons they can share at home with their families.

At the same time, it's good policy to 1) provide important information digitally to the families of your students – especially for those in elementary school and, *separately*, 2) send out content directly to your middle school and high school students as it relates to classwork, assignments and other relevant school information.

For families, including parents and guardians, it is OK if they are not tech-savvy. If there is something they don't understand, encourage them to reach out to other parents, to their child's school, or trusted family members. The goal here is not to make them or the student a security expert, but to make online learning a safe space.

For more information about how you can assess your cybersecurity knowledge as an individual or an organization, visit www.in.gov/cybersecurity/3826.htm.

***SHARE THE FOLLOWING ARTICLES WITH STUDENT PARENTS & GUARDIANS INCLUDING YOUR LOCAL PARENT SUPPORT GROUP OR PARENT TEACHER ASSOCIATIONS VIA EMAIL, NEWSLETTERS, ANNOUNCMENTS, ETC. THROUGHOUT THE SCHOOL YEAR.***

# *Article 1:*
# *Keeping Your Child Cyber Safe at Home*

With so many changes in the last several months, it has become even more important for families to make their homes more secure when connecting online for school and work.

As families, including parents and guardians, try to navigate these more virtual times, it is OK if they are not tech-savvy. If there is something you don't understand, reach out to other parents, to your child's school, or trusted family members. The goal here is not to make them or the student a security expert, but to make online learning a safe space.

The National Cybersecurity Alliance offers eight tips to share with families, including:

- NEW TECH? If the school issues or requires a technology that you and/or your child are not familiar with, explore its features together. Configure the security and privacy settings together immediately.

- APPLY YOUR RESEARCH. Apps are a great way for students to learn and apply their knowledge. Before downloading any new learning app on your child's device, make sure it is a legitimate app. Who created the app? What do the user reviews say? Are there any articles published online about the app's privacy & security features (or lack thereof)?

- DON'T HESITATE TO UPDATE. Having the latest security software, web browser, and operating system on devices children are using for their virtual schooling is one of the best defenses against online threats. When the computer or device says it's time to update the software, don't click postpone. Update.

- STRONG PASSWORDS IN PLAY KEEP CYBER CRIMINALS AT BAY. When is the last time you changed your home's router password, if ever? Change passwords for routers and smart devices from their default manufacturer's password to one that is long (at least 12 characters) and unique.

- PARENTAL CONTROLS. Parental controls are a great way to establish parameters around what kids can and can't do online. They do not replace candid discussions with your kids about online security and safety. Children may not recognize the dangers of visiting unknown websites or communicating with strangers online, so talk with them about these threats.

- NETWORK SEPARATELY. Students are not the only ones spending more time on the home network. Parents are also working from home at an unprecedented scale. *If you and your children are all working from home, consider using separate networks to enhance your security--particularly if your work involves access to sensitive information.*

- KNOW YOUR ROLE. Sometimes it is unavoidable for children to use the same computer that parents use for their work. If you are sharing devices, set up different user accounts so that children have access to a guest account with limited permissions and access. For instance, restrict your child's ability to install and run software applications.

- CONFIGURE PRIVACY SETTINGS. Go through accounts with children to configure privacy and security settings to limit over-sharing of information--such as location and camera sharing. Walk the kids through why certain settings need to be changed.

For additional resources, visit www.in.gov/cybersecurity/3832.htm.

# *Article 2:*
# *Keep Your Elementary Student Cyber Safe*

Elementary students have grown up surrounded by electronics and the internet. From games and videos on a tablet to synchronous Zoom calls with their third-grade class; young students are subjected to cyber risks everywhere.

Incorporating good cyber habits at a young age, particularly as the workforce becomes more embedded in the internet, will prevent hacks, theft, and fraud in the future.

Parents are the guiding force when it comes to teaching kids how to be safe when they are online. Introducing good cyber habits can be as simple as playing fishing games to teach about the dangers of "phishing" scams. Here are a few examples of how to teach cybersecurity tips to children, and how parents can protect children:

- Understanding passwords: It can become a habit, especially in children, to create one "master password" for all devices and accounts to make them easy to remember. And while passwords are often controlled and created by parents rather than children, it is important to ingrain the concept of having unique and *complicated* passwords for all accounts and devices to protect information.

- The App Store: There are thousands of apps and games that can be accessed through tablets, computers, and cell phones. However, not all of these are meant for children. Be sure that content restrictions are set in place through online accounts to ensure that only kid-friendly content is in the hands of kids.

While children may not seem like a main target of bad actors, they can be vulnerable. Child activity on unprotected networks can be a gateway for the bad guys to sensitive information such as financial records or other data. It is important to introduce these concepts early so that both you and your children can remain safe.

# *Article 3:*
# *Keep Your Middle School and High School Student Cyber Safe*

Just as they did while in elementary school, students, today, are familiar – and somewhat tech-savvy – when it comes to computers and being online, both for schoolwork and socially.

And, as students become teenagers, they are more likely to go places without their parents or even an adult. The same is true with the amount of time middle and high school students spend on their laptops, tablets, and phones.

Working with your child is key, especially as it involves being aware and having conversations with them about the sites they are visiting and who they are communicating with.

Tips include:

- Understanding passwords: It can become a habit, especially in children, to create one "master password" for all devices and accounts to make them easy to remember. And while passwords are often controlled and created by parents rather than children, it is important to ingrain the concept of having unique and *complicated* passwords for all accounts and devices to protect information.

- Protecting personal information on social media: It can be tempting to make funny posts on TikTok that reference the names of friends, names of schools, etc., but this can be incredibly dangerous. Social media is the newest form of communication for kids and adults alike, but it's also an easy way for people to gather information that can be used by bad actors for a variety of things. It's important to teach kids that personal information is *personal* and shouldn't be shared online.

- The App Store: There are thousands of apps and games that can be accessed through tablets, computers, and cell phones. However, not all of these are meant for children. Be sure that content restrictions are set in place through online accounts to ensure that only kid-friendly content is in the hands of kids.

While children and teens may not seem like a main target of bad actors, they can be vulnerable. Adolescent activity on unprotected networks can be a gateway for the bad guys to sensitive information such as financial records or other data. It is important to introduce these concepts early so that both you and your children can remain safe.

# *Article 4:*
# *Nine Ways to Cope with Working from Home with Kids*

Even before the Pandemic began, it was not unusual for family members, working from home, to be sharing space with their children, who, upon arriving home from school, are starting on their homework and class assignments.

Within the past six months, the number of people working remotely increased dramatically and it is expected to likely grow as the impact of the Pandemic continues to impact everyone across Indiana and around the world.

To help working parents adjust to the "new normal" a recent MSNBC article highlighted 9 tips for parents working at home with children (https://www.cnbc.com/2020/03/17/working-at-home-with-kids-during-covid-19-crisis-with-kids-underfoot.html). Among the suggestions involving shared workspace, it is suggested:

1. **Be upfront about expectations**. It's important to proactively communicate with your employer that your children are at home so they are aware that you cannot guarantee your work or work calls will be interruption-free. This applies to children as well: Explain to them that working from home means you really are trying to do work. While it may seem like a regular weekend or a vacation day because you are all at home, these are highly unusual circumstances.

2. **Set up virtual babysitters.** Reach out to friends, aunts, uncles, grandparents, babysitters, teachers. These individuals are amazing resources, because you can use them to arrange virtual playdates for your kids. They can talk, read, play games, sing, do dances and much more, all online.

3. **Plan activities that don't need supervision.** Different activities apply to different age groups, of course, depending on your schedule and the age of your children. While babies will give you a breather during nap times, you can rely on swings and bouncy chairs or put on music or Baby Einstein. Create activity boxes that contain games and puzzles that require minimal adult supervision for toddlers and grade-schoolers. Older kids will most likely be busy with online schooling.

4. **Prioritize your schedule.** Aim to schedule your most engaging/reliable activities for the kids to be on their own during the time you need to be most productive.

5. **Split the work.** If you have a partner, and if your work allows, you may consider taking shifts. For instance, one person watches the kids in the morning while the other works, and vice versa in the afternoon. This can better guarantee at least some hours where your focus is purely on work.

6. Reward good behavior. Working from home with kids means maintaining harmony however possible, and this includes setting up a reward system for them when they follow directions.

7. Take mini breaks. Consider temporarily changing your style of working. Instead of tackling a project for three hours, break up the day more to give your children the attention they need. Honor the fact that their attention spans are short, so your work will likely need to be done in chunks. Expect that you may need to continue working after they've gone to bed or wake up earlier in the morning to get more uninterrupted hours in.

8. Stress less about screen time: Under normal conditions, many parents limit screen time. It is worth considering adding to their daily screen time allotment to buy you more work time. Just explain to your children, though, that it is a temporary adjustment.

9. Get creative with office space. Try to find a space with a door that can be closed. Creating physical boundaries can help reinforce the message that you need to be working. Anyplace in the house with internet access can act as an office during an emergency, especially for when you have to ensure calls are uninterrupted.

# *Article 5:*
# *The New Normal — Sharing Your Workspace with Your Kids*

Growing up, it was bit of a big deal if you had an opportunity to go to the "office" with your Mom or Dad. The experience might have had a bit of a mystique to it.

Fast forward to earlier this spring, as the Pandemic began to take hold, the mystery was solved, as many companies sent their employees home to work remotely. And, at the same time, schools shifted from in-person, classroom instruction to e-learning at home.

Now, as a lot of families prepare to continue sharing space, working from home while your kids do their homework *is* the new normal. That said, there are a few things to keep in mind as you prepare for what, more and more, could become a way of life for some time to come.

When it comes to setting up an office, one of the first things that usually your company takes care of is the cybersecurity. But, when you work from home, you'll want to pay close attention to a few important tips, including:

- Always practicing good cyber hygiene by using antivirus software
    - Unfortunately, cyber threats are not on a pause. In fact, there is a clear spike in phishing and other cybercrime activity now that most people are working from home.
    - Make sure your systems and programs are up to date
- Ensure your home network is encrypted
    - Make sure, too, your router is protected with a secure password and if your router is more than 2 years old, you will want to replace it to provide the best protection
- Ensure your privacy with a Virtual Private Network (VPN) preferably issued by the company) to make sure your connection is protected along with your data and ALWAYS use it when connecting to a public Wi-Fi network
- Avoid oversharing your screen, especially during any online meetings and be sure that you haven't left any windows open with content that you wouldn't otherwise share. The same protection is there for any company information that might be proprietary
    - Be sure to maintain the same privacy, as it regards your children's schoolwork, along with any discussions you have online with their teachers and that it does not conflict with your work (i.e. online meetings)
- Beware of COVID-19 related scams, as It has been the topic of numerous international and national phishing and scam campaigns. If you get emails with any suspicious links or attachments related to Covid-19, don't open them

- Be sure not to share any personal information in messages, emails or on social media and make certain that the person requesting any information really did so before sending out what is known as PII – personal identifying information
    - It is also a risk to share pictures of your remote working station in social media. You might accidentally share important information while you do it.
    - Same is true with using your webcam. With webcams, you might also accidentally share too much about your home or your family members.
- Create a safe, comfortable environment for your kids – and yourself
    - As part of the approach, consider allowing your kids additional screen time, with the understanding that it is not a permanent situation, but they'll appreciate experiencing some added flexibility
- Working from home requires changing your routine and make sure your cybersecurity is part of that.

For additional resources, visit www.in.gov/cybersecurity/3832.htm.

# *Article 6:*
# *Working Remotely – How to Be Safe, Secure, And Successful*

Between working at the office, or school, or remotely, the principles of security can become something of a moving target. For some, this creates an uncertainty with making sure that the right policies are applied. Reducing risk on at-home networks, keeping information secure during virtual meetings and having a strong password policy are some best practices that can be implemented quickly and effectively from wherever you are working.

## *REDUCING RISK ON HOME NETWORKS*

Home IT devices, such as unsecured off-site routers, modems, and other network devices are subject to many of the same threats as on-site business devices. They can be attacked from any device on the internet. Remote devices are also vulnerable to unauthorized access from neighbors and passersby.

As we continue to work, attend school, and connect with friends and family remotely, there are steps you can take to reduce the risk and improve the security of home networks. Consider the following list to gauge the amount of risk involved and improve the security of your home network:

- Are your network devices physically secured?
- Have you changed the default manufacturer/administrative account password on your network devices (modem and router)? Many routers will come preconfigured with a password. The default password for most router models are easily accessible on the internet, making it extremely important to change the administrative passwords and not use the default.
- Do you have a unique password and two-factor authentication (2FA) enabled on your network devices (modem and router)?
- Do you have a password policy in place? Do you have a unique password and 2FA enabled on your internet service provider's web portal?
- If you use a mobile application for network management, do you have a unique password and 2FA enabled?
- Have you installed the latest updates for your network devices (i.e., modem, router, laptop/PC) or have you enabled auto-update with the device's administration page?
- Does your network device (router/modem) support Wi-Fi Protected Access Version 2 (WPA2) or Wi-Fi Protected Access Version 3 (WPA3)? WPA2 should be the minimum.
- Have you turned off/disabled Wireless Protected Setup (WPS) and Universal Plug and Play (UPnP) on your network? If enabled, these might allow attackers to connect to your devices without permission.
- Have you changed the Wi-Fi network name to something unique that doesn't provide any identifying information?

- Have you enabled firewall on your network devices?
- Have you disabled remote management? Most routers offer the option to view and modify their settings over the internet. Turn this feature off to guard against unauthorized individuals accessing and changing your router's configuration.
- Have you hardened your device by removing ports, software or services that are unused or unwanted?
- Do you run updated antivirus and malware protection on your device?

## *SECURITY DURING VIRTUAL MEETINGS*

In order to help protect you and your organization from potential threats, here are some cybersecurity tips on how to securely configure your virtual meetings, whether they be for work or your classroom experience.

### *Sharing of Your Information Assets During Virtual Meetings*

- Avoid adding your meeting to any public calendars or posting it on social media
- Require participants to enter an access code
- Avoid reusing access codes or meeting pins
- Distribute the meeting link and access code directly to the intended participants
- Remind invited guests not to share the access code
- Before sharing your screen, close unused windows to ensure you do not share sensitive or confidential information
- Use a privacy shield or cover over your webcam when it is not in use

### *Managing Your Information Assets and Password Policy*

- Use your organization's provided services and devices
- Do not record the meeting unless it is necessary and be aware that others may be able to record the meeting
- Disable the "Anyone Can Share" feature to prevent unauthorized screen sharing
- Muting users on entry can prevent potential disruptions
- Prevent users from sharing video by default; allow video sharing only when necessary
- Validate the participant list against invited attendees, or have participants identify themselves as they join the meeting
- Do not trust the safety of links shared in meeting chats
- Schedule "Unlisted" meetings and hide specific details, such as its host, topic, and starting time
- Do not allow attendees to "Join Before Host"
- Set up each meeting to require all attendees to enter a password
- Create a unique password comprised of upper, lower case, numbers, and special characters for each meeting

- Exclude the meeting password from attendee email invitations. Provide the password to attendees via a separate email or by phone
- On reoccurring meetings, always check to ensure one-time attendees are not included in subsequent meetings or meeting chat threads.
- Do not list personal information, such as location, phone number, or date of birth on your Skype profile

Remember, just like you protect your physical assets (shed, kayak, or bike) with a padlock, you need to lock down connectivity devices to protect information assets! A resilient cybersecurity mindset contributes towards being able to have a clear view of the objectives. For some, end points might have become a primary concern, for others, the corporate assets might have become even more susceptible in light of the increased amounts of ransomware. This dual pronged problem especially became more evident during this new world of COVID-19 with more staff working remotely.

Have you identified more risk than you initially realized? More information and mitigation techniques can be found at Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA).

# PROTECT YOUR STUDENTS

***SHARE THE FOLLOWING ARTICLES WITH STUDENTS VIA EMAIL, NEWSLETTERS, ANNOUNCMENTS, ETC. THROUGHOUT THE SCHOOL YEAR.***

## *Article 1:*
## *Protecting Yourself Online*

Whether you are a sixth grader entering middle school or a senior preparing for graduation, you have grown up surrounded by electronics of every variety and the Internet.

From games and videos on a tablet to completing your homework and engaging others on social media, you are online, often for hours at a time each day. And, while it's OK to have fun, whether you're on your laptop or phone, at school or at home, there are several things you can do to protect yourself from people who are looking to steal your identity or target you for abduction or worse.

Here are some helpful tips from Norton (a recognized authority on cybersecurity):

- Don't use the same password twice
- Direct messages from unknown accounts are usually not reliable. Report and block these accounts and be sure to *not* open any links they send.
- Avoid sharing too much personal information like where you live, your whole name, what time you are home alone, etc.
- Put a lock on your phone – a pattern, a code, facial recognition etc.; this will ensure that, if your phone is taken by another person, they cannot access your phone, personal data or your social media accounts.
- The block button is not something to fear! It will help keep bad people away from your information, keep you safe, and your feed uncluttered

For more, visit www.in.gov/cyber.

# *Article 2:*
# *Don't Get Hacked*

When you're at school or you are working on completing your class assignments, there are some important things you can do to make sure your computer is protected against viruses and hackers and you are not exposed to any sort of security risks (like someone hacking your microphone or camera to take illegal audio and video of you).

- Enable Automatic Updates so your computer is the most secure
- Shut down or restart your computer once a week to allow updates to take effect
- For all your devices, remember to backup your photos, documents, etc. in case you lose your device, or it gets hacked and you have to erase your device.
- Always install updates when your carrier tells you they are available
- Be sure to always use legal filesharing services for obtaining music, movies, TV, games, books, etc. on the Internet. A large list of digital music, videos, and other services is available from Educause at http://www.educause.edu/legalcontent. If you use illegal services, know that many people include links to malware to hack your computer.
- When you are not using your computer, turn it off. If you are using your computer, put a protective cover on your webcam so it *cannot* take pictures of videos without you knowing.

For more helpful tips for protecting yourself online, be sure to check out https://its.ucsc.edu/security/student.html. You can also learn to best protect yourself on social media, by looking over a *Social Media Guide* and additional resources at https://www.in.gov/cybersecurity/3830.htm.

# *Article 3:*
# *Top 5 Cyber Tips for To Start NOW*

Whether doing research, finishing assignments, emailing teachers or classmates, or just communicating, your computer and phone is a gateway to a lot of problems you don't need, especially now.

Here are five cybersecurity tips for students according to MYKI.com (a reputable digital identity management company):

## *1- Be careful what you share*

You might want to consider the impact of what you post online. We'd all like to show off that we passed our driving test, or that we're going on vacation, but posting pictures of things like driver's licenses, boarding passes, or credit cards makes you a prime target for identity theft.

## *2- Lock up and shut down*

Leaving your laptop or phone unlocked is a big mistake. The damage might be as minor as your annoying roommate changing your Facebook profile picture to something silly, or as major as some stranger in the cafe you're working at messing with your bank account. If you're going to leave your laptop or phone unattended, make sure you lock it, or set it to sleep or shut down after a certain period of inactivity.

## *3- Avoid phishing emails*

Think twice before you reply to that Nigerian prince.

There are plenty of thieves and scammers on the web, and phishing emails are one of their tried-and-true tactics. These are emails that might look like they're from a trustworthy source, but are actually trying to trick you into providing sensitive data, like your password or credit card details.

All you have to do to prevent yourself from being "phished" is have some common sense and make sure the sender of an email is really who they say they are.

## *4- Stick to HTTPS websites*

Here's something you may have never stopped to consider. Look up at the address bar of your browser: the URL begins with "https".

This means that unlike HHTP protocol websites, the site you're currently on uses a secure protocol, and all communication between your browser and that site is encrypted. In other words, no third party can eavesdrop on you and intercept the data you provide that site. That's not to say that all HTTP websites are malicious, but it's always best to proceed with caution.

## *5- Use a password manager*

Last but not least, you'll need to get yourself a good password manager.

On top of the dozen social media accounts you've already got, you're probably going to need some new academic accounts, which means a *whole lot* of passwords to remember.

But since you're only human, you'll be very tempted to use the same easy-to-remember password for everything, which is actually quite risky.

This is why it is highly recommended that you use strong and unique passwords, which you can securely store with a password manager.

For more information, visit www.in.gov/cyber.

# SOCIAL MEDIA CONTENT #4YOU2SHARE

Social media is a platform for learning, especially when it comes to cybersecurity.

And, whether you're sending out a Tweet, sharing a post on Facebook, or you have information to provide to others in the business world on sites, such as LinkedIn, it's important that you make sure you are communicating in a way that is safe and secure.

Although it is true that good advice can often be shared in as little as 40 characters or to a link that takes you to a credible source, so, too, it's important to follow best practices whenever you are online.

Here is some content and quick links we invite you to share with your family, friends, colleagues, and community members. You can use this content on your social media platforms or as part of any digital newsletters and other communication you are providing to families and students.

## *Content for Students*

- Read the *Social Media Guide for Students, Parents, and Bloggers* at https://www.cisa.gov/sites/default/files/publications/Social%20Media%20Guide_1.pdf

- Cyberbullying is not a thing of the past. Learn how young people can identify and protect themselves from cyberbullies here: https://www.us-cert.gov/ncas/tips/ST06-005 #cybersecurity #stopcyberbullying

- Cybersecurity Tips for Teens & Families: Things I Wish My Parents Had Told Me About Internet Safety. https://www.netliteracy.org/safe-connects/collateral-material/?gclid=EAIaIQobChMImZuxmZqR6wIVjsDACh3XIARIEAAYAiAAEgIBlPD_BwE

- Back to school season is coming right up! Pens and pencils are important, but so is staying cyber safe! Learn more student cyber safety here: https://securityboulevard.com/2019/08/back-to-school-tips-the-abcs-of-online-security/ #cybersecurity #backtoschool

- Series on Student safety
    - https://ets.hawaii.gov/wp-content/uploads/2016/09/Cyber-Tips-for-Students.pdf
    - https://www.us-cert.gov/ncas/tips/ST06-005
    - https://www.marquette.edu/remote-learning/cyber-security-tips.php. - remote learning

- Cybersecurity Tips for Student Bloggers https://staysafeonline.org/blog/cybersecurity-tips-student-bloggers/

## *Content for Parents*

- 5 Cyber Safety Tips Every Parent Should Know.

- Top 5 Questions Parents Have About Cybersecurity https://www.connectsafely.org/wp-content/uploads/securityguide.pdf

- Tips for Parents - Protecting Kids Online https://www.consumer.ftc.gov/topics/protecting-kids-online

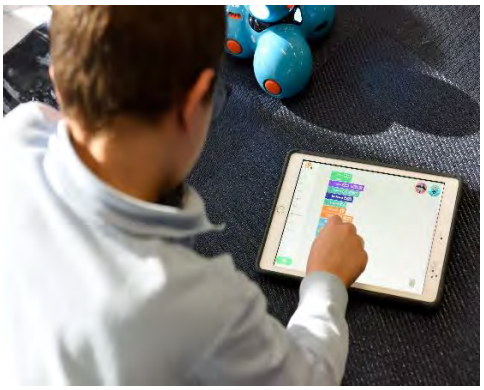
- 13 Apps Every Parent Should Know in 2020 https://educateempowerkids.org/13-apps-every-parent-should-know-in-2020 #cybersecurity

- Parents: With kids spending more time online, it is important to teach them how to be cyber safe. Learn more about social media safety here https://au.norton.com/internetsecurity-kids-safety-parents-best-practices-to-social-media-security.html #cybersafe #cybersecurity #cyberaware

- Tips for Parents Raising Privacy-Savvy Kids https://documentcloud.adobe.com/link/review?uri=urn:aaid:scds:US:09e0015f-3bc7-4504-b008-88692c8ef737

# *Images for Social Media*

As you use the social media content and develop your own content for your school district with the many tips in the *Cybersecurity for Education Toolkit*, feel free to copy and paste the below images with your messages.



# SCHOOL COMMUNITY PATRONS

Who are your school community's patrons? They are the people who help make up your town or city; everyone from your grandparents to that young couple who just moved in next door.

In other words, it is everyone who is *not* a student, teacher, staff member, administrator, or school board member. Yet, they are invested in living in a place that values education and understands that good schools contribute to the quality of life within the community.

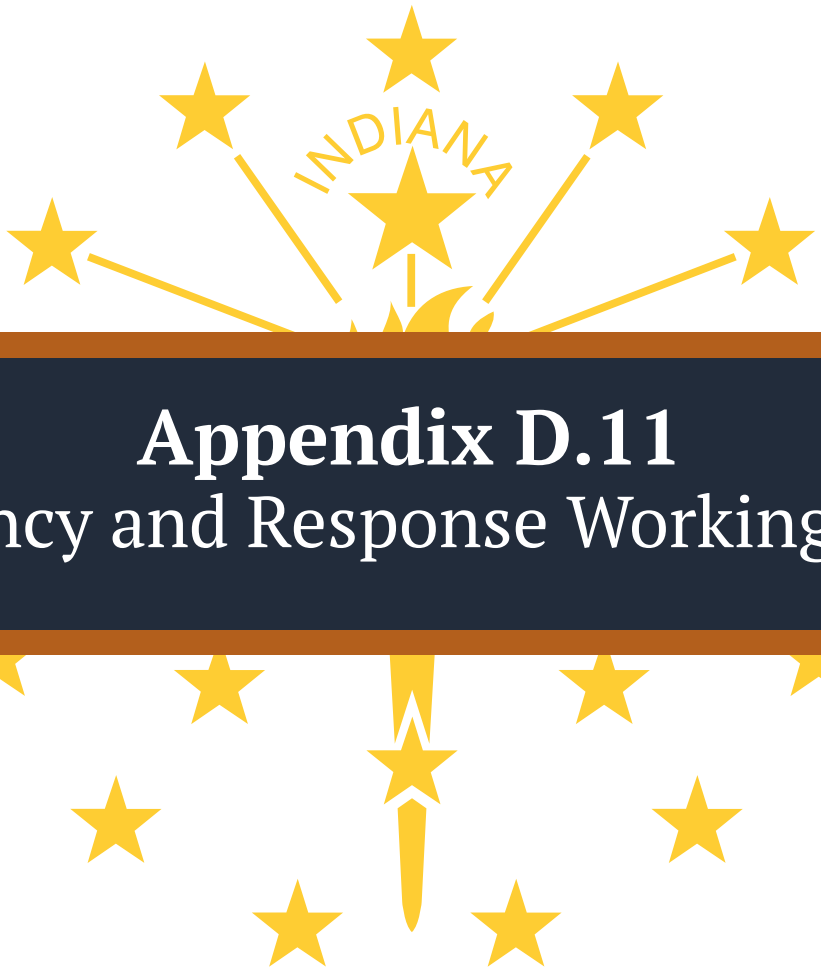
School districts routinely communicate information with people through newsletters, stories in the news media and through their family members and friends.

Because of this, it is important for members of the public to know and understand the importance of being cybersafe and there are resources out there for everyone.

STOP. THINK. CONNECT. ™ is the global online safety awareness campaign to help all digital citizens stay safer and more secure online. The message was created by an unprecedented coalition of private companies, non-profits and government organizations with leadership provided by the National Cyber Security Alliance (NCSA) and the APWG.

The campaign was launched in October of 2010 by the STOP. THINK. CONNECT. Messaging Convention in partnership with the U.S. government, including the White House. NCSA, in partnership with the APWG, continue to lead the campaign. The Department of Homeland Security leads the federal engagement in the campaign at:
https://stopthinkconnect.org/

For additional resources, visit www.in.gov/cyber.




# Appendix D.11
## Resiliency and Response Working Group

# RESILIENCY AND RESPONSE WORKING GROUP STRATEGIC PLAN

Chair: Adjutant General, Brigadier General Dale Lyles
Co-Chair: Executive Director Stephen Cox


October 2021
Indiana Executive Council on Cybersecurity

# Resiliency and Response Working Group Plan

# Table of Contents

# Committee Members

# Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Alley | Mike | Resilient Strategies, LLC | President | Full Time |
| Baldwin | Ashley | Indiana Department of Homeland Security | State Exercise Officer | As Needed |
| Barefoot | Jonathon | IU Health | Vice President | Full Time |
| Cox | Stephen | Indiana Department of Homeland Security | Executive Director | Co-Chair |
| Day | David R. | MISO Energy | Consulting Information Security Analyst | Full Time |
| Tooley | Benjamin | Indiana National Guard | J36 Defensive Cyber Programs | Full Time |
| Hackett | Jeffrey (Col) | Indiana National Guard | External Affairs and Alliances | Co-Chair Proxy |
| Justice | Connie (Dr.) | IUPUI | Professor | Full Time |
| Lucas | John | Citizens Energy Group | Vice President, IT | Full Time |
| Lyles | Dale (BG) | Indiana National Guard | Adjutant General | Chair |
| Moran | Mary | Indiana Department of Homeland Security | Response and Recovery Director | Full Time |
| Neel | David | CyberTek MSSP | Chief Technical Officer | As Needed |
| Musgrave | Anthony | Indiana National Guard | J36 Defensive Cyber Programs | Full Time |
| Reuter | Ed | Indiana Statewide 911 Board | Executive Director | As Needed |
| Rogers | Marcus | Purdue Polytechnic | Professor/Executive Director Cybersecurity Programs/Chief Scientist HTCU | As Needed |
| Rogowski | Peri | Indiana Department of Homeland Security | State Planning Director | As Needed |
| Romero | Joseph | IU Health | Emergency Preparedness Program Manager | Full Time |
| Skalon | Dave | Indiana National Guard | Chief Information Officer | Full Time |

| | | | | |
|---|---|---|---|---|
| Winslow (BG) | Timothy | Indiana National Guard | Director of the Joint Staff | Chair Proxy |
| Goldsmith | Reid | Indianapolis International Airport | Senior Director Information Technology | As Needed |
| Mackey | William | Indiana State University | Instructor | As Needed |
| Dignin | Kelly | Integrated Public Safety Commission | Director of Network Services | Full Time |
| Ferrante | Anthony | FTI Consulting | Global Head of Cybersecurity, Senior Managing Director | As Needed |
| Potchanant | Joe | Indiana University REN-ISAC | Director of Member Services and Support | As Needed |
| Pelletier | Ronald W. | Pondurance | Founding Partner | As Needed |
| Aikman | J. Kurt | MISO Energy | Senior Security Advisor | As Needed |
| Linder | Jared | Family and Social Services Administration | Chief Information Officer | As Needed |
| Vare | Todd | Barnes & Thornburg LLP | Partner | As Needed |
| Redman | Justin | Citizens Energy Group | Manager Water System Control and Planning | As Needed |
| Neely | Dewand | MGT Consulting | Chief Information Officer | As Needed |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan.*

For more information, visit www.in.gov/cybersecurity.

# Executive Summary

# Executive Summary

- **Research Conducted**
  - **Cybersecurity and Infrastructure Security Agency (CISA):** CISA leads the Nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services and American way of life.
  - **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):** Helping organizations to better understand and improve their management of cybersecurity risk.
  - **National Institute of Standards and Technology (NIST) Risk Management Framework (RMF):** The NIST Risk Management Framework (RMF) provides a comprehensive, flexible, repeatable, and measurable 7-step process that any organization can use to manage information security and privacy risk.
  - **Multi-State Information Sharing and Analysis Center (MS-ISAC):** The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.
  - **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.

- **2018 Pre- thru Post- Cyber Incident Working Group Primary and Secondary Research Conducted:**
  - Each of the sector sub-groups was tasked to create a white paper 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 2017, the team has 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.
  - The team also have been exploring the idea of conducting a "GRIDEX-like" exercise for both the water/wastewater and election sectors.

- **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.
  - The NIST Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.
  - There is an abundance of cybersecurity information and services and resources available to individuals, government agencies, and private sector organizations.
  - Within the past few years, the ability to conduct self-assessments for cybersecurity risk have made improvements. The NIST CSF provides a list of several free tools to assist small to medium sized business (SMB) conduct internal reviews.
    - https://www.nist.gov/cyberframework/assessment-auditing-resources
  - There currently is no central point of coordination and information sharing for state-level cybersecurity planning, training, and exercise activity.
  - There currently is no centralized point for reporting cyber incident attacks occurring within the State of Indiana and coordination is required among various agencies to respond.
  - Incident Response support of federal or state resources is agency dependent based upon the attack victim’s line of business (healthcare, financial, local government, state government, or whether a crime has been committed).

- **2018 Pre- thru Post- Cyber Incident Working Group Primary and Secondary 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 to coordinate response and prevention. 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 are valuable 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" method of outreach and training thru sector exercises would be a better use of these limited resources and farther reaching than a penetration assessment alone.
  - We would recommend that the IECC strongly consider developing outreach, training, and exercises for other Sectors.

- **2021 Working Group Deliverables**
  - Exercise
  - Cyber Emergency Response Team (IN-CERT)
  - Emergency Manager Cybersecurity Toolkit 3.0
  - Cyber Annex and Cyber Liaison
  - INNG Cyber State Capabilities

- **Additional Notes**
  - No additional information at this time.

- **References**
  - Cybersecurity and Infrastructure Security Agency (CISA)**:** https://www.cisa.gov
  - National Incident Management System (NIMS): https://www.fema.gov/national-incident-management-system
  - Emergency Management Accreditation Program (EMAP): https://www.emap.org/
  - National Institute of Standards and Technology (NIST): Risk Management Framework (RMF): https://csrc.nist.gov/Projects/risk-management/
  - National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): https://www.nist.gov/cyberframework
  - Multi-State Information Sharing and Analysis Center (MS-ISAC): https://www.cisecurity.org/ms-isac/
  - 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
- American Water Works Agency: https://www.awwa.org/

# Research

# Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
   - Efforts in cyber-preparedness include the following:
     - 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 and Exercise completes Cybersecurity Awareness Workshops for Emergency Management Administrators (EMAs) in districts 1, 2, 3, and 4.
     - Continuity/Cybersecurity workshops are brought into local jurisdictions, designed by Federal Emergency Management Agency (FEMA) and US DHS.
     - A Cyber Incident Response Annex was completed November 2019.

   - 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
     - CyberShield 2019
     - Homeland Defender 2021

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
   - Critical infrastructures and emergency service sectors
   - 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 must 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, and etc.

3. **What is your area's greatest cybersecurity need and/or gap?**
   - Resources to serve all those in need during a multi-event cyber response crisis.
   - 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**. Public Safety**
- The Working Group requested that the following authorities, as listed in the State of Indiana's Cyber Emergency Response Annex, review the following information 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.
    - 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
  - **State**
    - Cyber Security Framework Strategy For the State of Indiana
    - Indiana Code 10-14-3, Emergency Management and Disaster Law
    - A Leader's Guide to Emergencies and Disasters, IDHS
    - Executive Order 13-09, January 2013
    - Indiana Executive Council on Cybersecurity
  - **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 Department of Homeland Security (DHS) Critical Infrastructure (CISector 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 question #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.
   - 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.
   - The Working 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 answering 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.

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

- The Working 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: State Cyber Exercises

# Deliverable: State Cyber Exercises

## *General Information*

1. **What is the deliverable?**
    a. State Cyber Exercises
        i. INCyber TTX – Aug. 11, 2021
        ii. Indiana Homeland Defender – Aug. 13, 2021
        iii. Indiana Homeland Defender – 2023

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?**
☐ 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. State Cyber Exercise 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?**
☒ 2021 ☐ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

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. Indiana Office of Technology (IOT), Indiana Department of Homeland Security (IDHS), Indiana State Polis (ISP), and Indiana National Guard (INNG)

12. **Who should be main lead of this deliverable?**
    a. Cybersecurity Program Director and INNG

13. **What are the expected challenges to completing this deliverable?**
    a. Completing with current resources and communicating the new program to stakeholders who would benefit.

# *Implementation Plan*

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

☐ One-time deliverable

☒ Ongoing/sustained effort

## Tactic Timeline

**INCyber CISA Exercise – August 11, 2021**

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review and Finalize Cyber Annex | Cybersecurity Program Director/IDHS/IOT/ISP/INNG | 100 | Nov. 2019 | |
| Work with USDHS CISA on planning the scenario | Cybersecurity Program Director/IDHS/IOT/ISP/INNG with USDHS CISA | 100 | December 2020 | |
| Prepare with planning partners in initial, mid, and final planning meetings | USDHS CISA and IECC partners | 100 | Jan-July 2021 | |

| | | | | |
|---|---|---|---|---|
| Hold Exercise | USDHS CISA and IECC partners | 100 | Aug. 11, 2021 | |
| Review AAR | Cybersecurity Program Director and USDHS CISA | 100 | October 2021 | |

**INNG Homeland Defender Exercise – August 13, 2021**

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Update INNG "All Hazards" Plan | INNG J3 | 100 | Sep. 2021 | INNG force packages to respond to state emergencies |
| Exercise County EOC IR Processes | IDHS | 100 | Aug. 2021 | Johnson County EOC |
| Initiate cyber IR component to future exercises | IDHS | 100 | Aug. 2021 | |
| Exercise 1st responder TTPs | Multi-Agency | 100 | Aug. 2021 | |

***Homeland Defender II – 2023**

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Exercise joint civilian and military Critical Infx response exercise | INNG J36 and IDHS | 0% | Aug. 2023 | -EOC Command<br>-IDHS Cyber Fusion Cell |
| Exercise County EOC IR Processes using Emergency Manager Cybersecurity Toolkit 3.0 | IDHS | 0% | | See deliverable below |
| Physical breaches | MUTC | | | Physical Location |
| IT/OT defense | MCTC | | | Cyber Range |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1 | | Exercise Planner | Mix INNG and State | DHS and CISA | IDHS SEO (A. Baldwin) or CISA |
| 1 | | Project Officer | INNG | | Will need to manage on-site coordination and range scheduling at MUTC |
| 3 | May require external vendor or IECC partner with range (Purdue?) | IT Virtual Environment | Unknown | Unknown | Need to develop virtual environment (range) to defend which mimics a city or county administration office |

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

a. No Response

| 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

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

a. The Exercises 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. Not having a reviewed, trained, and exercised a cyber incident response plan can have a high impact (and cost) 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?**

☐No ☒ Yes

a. Yes, at varying levels. Requires more research and decisions by working group.

**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. Several other states conduct exercises with partners.

## Other Implementation Factors

---

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

a. Staff, monetary resources, or administrative priorities could change or slow the timeline of the project down. For INNG, legal and financial review of federal funds used in combined training exercise will be required. DHS or CISA may be able to fund without constraints.

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

☐No ☒ Yes

a. Perhaps a change in internal agencies with 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. Water and Wastewater Committee as well as the Healthcare Committee

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes,

a. 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)?**

☒No ☐ Yes

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

a. It is important to always the benefit of communicating about the success of an exercise while not over sharing for bad cyber actors to take advantage of in the future.

## *Evaluation Methodology*

**Objective 1:** The State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Table Top Exercise by August 2021.

*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 work with INNG to incorporate a cyber attack into a natural disaster exercise during the Homeland Defender Exercise by August 2021.

*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:** The State of Indiana will develop and execute a Cross-Sector Critical Infrastructure Cyber Operational Exercise by 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

# Deliverable: Cyber Emergency Response Education to Local Law Enforcement

# Deliverable: Cyber Emergency Response Education to Local Law Enforcement

## *General Information*

1. **What is the deliverable?**
    a. Cyber Emergency Response Education to Local Law Enforcement

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?**
☐ 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 purpose of Cyber Emergency Response Education to Local Law Enforcement Fact Sheet is to inform local agencies so that when a cyber attack occurs, they are educated about who to call and when.

6. **What metric or measurement will be used to define success?**
    a. Completion of the education materials and distribution to local law enforcement agencies in Indiana.

7. **What year will the deliverable be completed?**
☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. local government and law enforcement agencies

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. ISP, IDHS, IOT, FBI, USDHS, US Secret Service

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. State and Local Government Committee and Cyber Awareness and Sharing 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. ISP, IDHS, IOT, FBI, USDHS, US Secret Service

12. **Who should be main lead of this deliverable**?
    a. ISP and Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. Resources and coming to a consensus of the proper steps in a response between state and federal agencies where appropriate.

## *Implementation Plan*

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

☒ One-time deliverable

☐ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Draft Info Sheet | Cybersecurity Program Director and ISP | 0% | February 2022 | |
| Edit and provide to partners for feedback | Cybersecurity Program Director and ISP | 0% | March 2022 | |
| Finalize | Cybersecurity Program Director and ISP | 0% | May 2022 | |
| Distribute | ISP with IECC partners | 0% | June 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

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

a. No Response

| 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?**

a. When a cyberattack occurs, the efficiency and speed of notifying law enforcement agency who is the most appropriate given the organization affected by the attack is imperative especially for attacks that may cause harm.

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

a. It may reduce any initial confusion of requesting enforcement agencies

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

a. If there is confusion of who to contact when, we could have the potential of an organization not receiving the law enforcement assistance and dire secondary consequences could occur as a result of the attack.

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

a. In addition to completion of the deliverable, increasing awareness of local law enforcement agencies.

**21. 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. Other states have been working on communicating with local law enforcement agencies, but they are usually very specific and specialized guidance. Not currently aware of a proactive campaign in other states as of now Other states have been working on communicating with local law enforcement agencies, but they are usually very specific and specialized guidance. Not currently aware of a proactive campaign in other states as of now

**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?**

☐No ☒ Yes

a. There are several federal agencies that have provided similar guidance. There are several federal agencies that have provided similar guidance.

## Other Implementation Factors

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

a. Shifting priorities or disagreement of steps and resources being provided to local law enforcement agencies.

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

☒No ☐ Yes

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

a. It will require a regular review by ISP and the Cybersecurity Program Director

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

a. State and Local Government Committee

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

## Communications

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

a. Local government organizations and law enforcement agencies

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

☐No ☒ Yes

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

a. Not at this point.

## *Evaluation Methodology*

**Objective 1:** Indiana State Police and Cybersecurity Program Director work to develop the Cyber Emergency Response Education for Local Law Enforcement by May 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

**Objective 2:** Indiana State Police and IECC partners distribute the Cyber Emergency Response Education to 80 percent of Local Law Enforcement by June 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: Emergency Manager Cybersecurity Toolkit 3.0

# Deliverable: Emergency Manager Cybersecurity Toolkit 3.0

## *General Information*

1. **What is the deliverable?**
    a. Update the state's Cyber Incident Planning and Preparedness Toolkit for Emergency Managers that is compliant with FEMA, USDHS, and NIST.

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?**
☐ 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. 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?**
☐ 2021 ☐ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review current resources and templates for incident response toolkit | Resiliency and Response Working Group | 25% | December 2021 | |
| Make edits to toolkit – version 3 | Cybersecurity Program Director | 0% | February 2022 | |
| Develop cyber workshops | IDHS | 0 | January - March 2022 | |
| Conduct cyber workshops | IDHS | 0 | March 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1.0 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 |
|---|---|---|---|---|---|---|
| No Response | | | | | | |

## 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 are 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?**

☐No ☒ Yes

a. Small Business Administration, Federal Communications Commission (FCC), and FEMA have templates to use in incident response planning. 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?**

☐No ☒ Yes

a. 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. information technology and emergency management. 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 require a high knowledge in information technology and emergency management. 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 require a high knowledge in i

## 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?**

☐No ☒ Yes

**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?**

☐No ☒ Yes

a. All sectors would benefit

## 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)?**

☐No ☒ 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 update the Emergency Manager Cyber Response Toolkit 3.0 by March 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

**Objective 2:** IDHS will launch a workshop using the Emergency Manager Cyber Response Toolkit 3.0 by April 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 Annex and Cyber Liaison

# Deliverable: Cyber Annex and Cyber Liaison

## *General Information*

1. **What is the deliverable?**
    a. Finalize IDHS Cyber Annex and train cyber liaisons

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?**
    a. Update 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? 2018**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. State and Local Government 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), 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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review Annex from IDHS – Preliminary review with key stakeholders | Cybersecurity Program Director/IDHS/IOT/ISP/INNG | 50 | Qtr. 1 2022 | |
| Edit Annex and review with partners | IDHS | 0 | Qtr. 2 2022 | |
| Finalize and Distribute Annex | IDHS | 0 | Qtr. 3 2022 | |
| Train CLO | IDHS/IOT | 0 | Qtr. 4 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

**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. 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 are 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 the review of the 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?**

☐No ☒ Yes

a. The National Governor's Association and FEMA identified several other states who have a cyber annex. The National Governor's Association and FEMA identified several other states who have a cyber annex. 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?**

☐No ☒ Yes

a. The National Governor's Association and FEMA identified several other states who do not have a cyber annex.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?**

☐No ☒ Yes

**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. None at this time.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. All critical infrastructure sectors 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)?**

☒No ☐ Yes

**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 edit and distribute the IDHS Cyber Annex to appropriate parties by Qtr. 3 of 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

**Objective 2:** IDHS and IECC partners will exercise the IDHS Cyber Annex with the cyber liaisons 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

# Deliverable: INNG Cyber State Capabilities

# Deliverable: INNG Cyber State Capabilities

## *General Information*

1. **What is the deliverable?**
   INNG Cyber State Capabilities

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?**
   The Indiana National Guard is prepared to provide cyber response capabilities to a statewide cyber emergency when directed by a Federal disaster declaration or ordered to State Active Duty by the Governor.

6. **What metric or measurement will be used to define success?**
   Establishment of escalation and notification criteria and processes between the IDHS and the Indiana National Guard to include Memorandums of Agreements.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☐ 2022 ☐ 2023 ☒ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   IDHS and the Indiana National Guard.

9. **Which state or federal resources or programs overlap with this deliverable?**
   CISA, FBI, DoJ, and the ISP

## 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?**
    IDHS and the Indiana National Guard.

12. **Who should be main lead of this deliverable?**
    IDHS Directory and the Adjutant General of Indiana.

13. **What are the expected challenges to completing this deliverable?**
    Current U.S. Federal law has restrictions for use of Title 32 forces and equipment to support state emergency response. Activation of the National Guard by the Governor to support cyber incident response activities requires legal review and guidance for activities NG soldiers would perform on state or local government networks.

# *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| IDHS Cyber Annex to the CEMP | IDHS | 0% | 2022 | |
| INNG All-Hazards Cyber Response | INNG | 75% | 2024 | |
| Legal Review, NDA, MOA | Indiana Attorney General and INNG Judge Advocate General | 0% | 2024 | |

| | | | | |
|---|---|---|---|---|
| Passage of the National Guard Cybersecurity Act | U.S. Congress | | | |

## Resources and Budget

**15. 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 |
|---|---|---|---|---|---|---|
| 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.)**

The National Guard would have the regulatory and legal clarification to provide active support during a large-scale cyber emergency.

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

The INNG would be able to provide response forces to bolster the efforts of CISA, the FBI, or the IDHS when responding to cybersecurity related incidents. The costs would be dependent upon the size of the force requested and the duration of the event.

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

INNG response forces remain limited to an advisory role.

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

A co-developed MoA between IDHS and the INNG.

**21. 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. Texas.

**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?**

☐No ☒ Yes

## Other Implementation Factors

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

a. Failure to pass the National Guard Cybersecurity Act would continue ambiguity of response capabilities due to overlapping laws, DoDI guidance, and regulations.

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

☐No ☒ Yes

a. Passage of the National Guard Cybersecurity Act would allow the INNG to response to Cyber disasters similar to natural disasters.

**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. The National Guard is having internal discussions on how to develop this initiative.

**27. Can this deliverable be used by other sectors?**

☐ No ☒ Yes

## Communications

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

a. No Response

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

☒ No ☐ Yes

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

a. No Response

## *Evaluation Methodology*

**Objective 1:** The Indiana National Guard will inform state leadership of their cyber response capabilities to a statewide cyber emergency when directed by a federal disaster declaration or ordered to State Active Duty by the Governor by December 2024.

*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 Cyber Exercise – News Release and News Coverage
- Muscatatuck Urban Training Center – Homeland Defender Info Sheet
- Indiana Emergency Manager Cybersecurity Toolkit 2.0
- Indiana Cyber Emergency Resiliency Response State Guide
- Integrated Preparedness Information Handout

# Indiana Cyber Exercise
# News Release and News Coverage

# Indiana's Cyber Readiness Advancing Rapidly

Friday, October 1, 2021

If you think about it, protecting a school, hospital, or a city's water supply from a cyberattack is a lot like a football coach drawing up a game plan for playing against the #1 team in the country – every day.

There's game film, playbooks and you always have to account for how you're going to stop the other team's best player from scoring; all the while trying to figure out what else the coach might have up his sleeve. And there's no halftime show to try and adjust to stage a comeback.

That's the challenge facing the State of Indiana in its efforts to continue rapidly moving forward in its mission to further strengthen its cybersecurity resiliency and response.

The progress that's been achieved comes as the State of Indiana and the Indiana National Guard recently hosted two cyber exercises in a partnership with several federal agencies, health care providers, and technology companies, water utility service providers, state, and local government officials, as well as state and federal emergency and law enforcement agencies.

"Conducting these exercises highlights the strength of the cybersecurity structure that exists within the state and underscores the work that's been accomplished over the past three years by

Indiana Governor Holcomb's Executive Council on Cybersecurity with our partners in the military, academic, public and private sectors," said Indiana Department of Homeland Security Executive Director Stephen Cox. "Most importantly, it represents the progress with cyber that's been achieved on behalf of all Hoosiers when we approach cybersecurity as something that is not solved by one entity alone, but by everyone at all corners of the state."

Having a playbook is especially crucial, given the fact there are not only a seemingly endless number of situations in which a cyberattack or incident can occur, but there are all kinds of circumstances and variables that can interfere with a cyber team's strategy for protecting its systems.

**When Water Runs Out…**

A water utility being attacked is not only scary to every city in America, but the reality of it also happening is real.

The Cybersecurity and Infrastructure Security Agency (CISA) has partnered with the State of Indiana and the City of Fort Wayne to exercise how state, federal, mutual aid, and local government would work together in a long-term cyberattack that eliminates the supply of water from the city, with a special emphasis on the secondary effects for the city's hospitals.

As the Cybersecurity Program Director for the State of Indiana, there's no question cybersecurity impacts every aspect of our daily lives. As we've seen with recent cyber incidents – everything from pipelines to water utilities to schools and hospitals – a cyberattack can create substantial effects and damage to our community and our critical infrastructure, disrupting our daily lives and safety.

**When Natural Disasters Hit…**

Following the completion of the tabletop exercise, a second cyber exercise as part of a full-scale functional exercise hosted by the Indiana National Guard for first responders and several military branches as well as search and rescue teams at the Muscatatuck Urban Training Center.

The grounds of the 1,000-acre facility, located in Southern Indiana, is a real city that includes a built-in physical infrastructure, a well-integrated cyber-physical environment, an electromagnetic effects system and human elements. There are more than 190 brick-and-mortar structures with roughly 1.5 million square feet under roof, 1.8 miles of subterranean tunnels, a cave complex, more than nine miles of roads, managed airspace, a 185-acre reservoir, and a cyber live-fire range.

The focus of the Indiana National Guard exercise centered on measuring how federal, state, local and private sectors respond to a devastating earthquake.

"We really need to prepare now for these acts which we've already seen here in Indiana and across the world," said Ron Pelletier, founder and chief customer officer at Pondurance, a cyber security company.  "When natural disasters hit all parts of the world, we are seeing more and

more targeted cyberattacks in those affected areas. Investing now in preventative measures is the best way to avoid situations like that from becoming worse. It comes down to planning to avoid cyber breaches but being prepared to respond."

As emergency and military teams respond to the effects of the earthquake, the Indiana National Guard also tested the additional response of its incident command leadership while the cyber experts from IU Health, Citizens Energy Group, and Pondurance made the efforts more difficult by attacking the water supply in the aftermath.

**It's Not "If" But "When"...**

Pelletier added that Pondurance hopes disaster drills, such as these two, will raise awareness among policy makers to help fund security programs and protocols. "National, state, and community security is truly at risk here, and we need to take action now to preserve it. Waiting for the dam to burst before you repair it is a terrible maintenance strategy, and that's exactly the situation we have here across power grids, water supplies, healthcare, you name it."

Having the ability to draw on the resources and expertise required at a moment's notice to keep people safe in the event of a cyber incident or attack relies on making certain that the state and its partners have a line of communications that's always open to make sure the State of Indiana provides a response that's most effective, regardless of the circumstances.

Many of those who are participated in both state exercises also serve on the Indiana Executive Council on Cybersecurity (IECC). As defined in Executive Order 17-11 from Indiana Governor Eric Holcomb, the IECC is a first-of-its-kind collaboration, whose work as an organization within state government, is responsible for guiding the state's cybersecurity policy, It is comprised of 35 Council members and 250 advisory members, all of whom are subject matter experts represent a wide range of businesses, industries and professions, including education, finance, utilities and insurance, among many others.

The State of Indiana and its partners offer best practices, guides, toolkits, and resources to allow all organizations and critical infrastructures to mitigate, but also prepare for a cyberattack. For more information about the IECC or the State of Indiana's Cyber Strategy, visit www.in.gov/cyber.

For more information about CISA's cybersecurity services and resources, visit www.cisa.gov.

LOCAL NEWS

# Indiana holds full-scale cybersecurity disaster drill

Lessons learned in the day-long drill at Muscatatuck will be used to help hospitals and utilities all across the state.

Indiana tests preparedess with cybersecurity disaster drill

Author: **Jennie Runevitch**
Published: **4:24 PM EDT August 17, 2021**
Updated: **7:49 PM EDT August 17, 2021**

MUSCATATUCK, Ind. — Hackers are increasingly hitting governments, utilities, and hospitals — critical infrastructure across the country — during severe storms or natural disasters.

That's why the state of Indiana just held a full-scale disaster drill to test and better prepare Hoosier response.

When a natural disaster strikes, damage from weather isn't the only threat anymore. Experts say right while we're at our most vulnerable, cyberattacks are now targeting hospitals, electric grids, and water systems.

It's happened a lot during hurricanes and wildfires and leaders in Indiana say it'll likely happen here, too.

"It is a staggering threat when we talk to our counterparts in Louisiana, in Texas, in Florida. When there are hurricanes coming at them, all of a sudden, they see the bad actors trying to get in their systems increase by a thousand-fold," said Chetrice Mosley Romero, the state of Indiana's Cybersecurity Program Director. "Bad actors watch the news and watch the weather channel just as much as the good people do, right? So, they're saying, 'hey - they're going to be affected. They're going to be distracted so we should go after that.'"

Enter "Operation Homeland Defender".

The massive cybersecurity drill, held over the weekend at Muscatatuck Urban Training Center, included the Indiana National Guard, local first responders, Indiana Task Force One, Indiana-based Pondurance, IU Health and Citizens Energy.

They conducted a simulated emergency, then injected a cyberattack.

*Credit: DVIDS via Indiana National Guard*

First, an earthquake hit, then in the chaos of trying to protect people and property, here come the hackers.

"So, we have people who come in and actually attack the water system and shut it down and now you have firefighters and rescue first responders who no longer have water," Mosley-Romero explained. "What can really make a bad day worse? Water's typically the top one."

Crews involved in the drill didn't know this was a cyberattack at first.

The exercise teaches that, so first responders know in the future that hackers are a possibility during disasters.

The groups also experience, in real time, how to plan and respond.

"So we have a red team that attacks the system and then we have a blue team who responds to that attack, closes up the system and then also educates the water utility on what they could've done to prevent the attack altogether," Mosley-Romero said.



Protecting health care and critical infrastructure, just when people need it the most, is the goal of this exercise.

Lessons learned in the day-long drill at Muscatatuck will be used to help hospitals and utilities all across the state.

"It isn't just one entity that solves it all, it is a 'all hands are on deck' situation because all of us are touching things that are plugged in, so all of us are really part of the cyber problem," Mosley-Romero said. "But we're also part of the cyber solution."

The state of Indiana has developed cybersecurity toolkits, for not only cities and businesses but also regular citizens.

You can even test yourself, to see how well you're protected. Find the information, tips and quizzes here.

**Related Articles**

**Attempted ransomware attack prompts Eskenazi Health to shut down systems and divert patients**

**New cybersecurity order issued for US pipeline operators**

**$10 million rewards bolster White House anti-ransomware bid**

PRESS RELEASES
STUDIES / REPORTS
MEDIA INQUIRIES / SPOKESPEOPLE
BIZVOICE MAGAZINE
MULTIMEDIA
BLOG





Previous Next

# COLLABORATION KEY AS INDIANA PREPARES FOR MAJOR CYBERATTACKS

September 29th, 2021

By Adam Berry

The U.S. military is used to fighting battles on the land and sea and in the air.

But now, there's a new battleground – in space. Cyberspace.

So when the Indiana National Guard prepares for natural and man-made disasters, you can bet they call in an ample supply of cybersecurity firepower. This summer, officials from the Indiana National Guard and state of Indiana conducted two drills to prepare for disasters and layered into the plan a new, higher level of cybersecurity.

That's because an emerging – and troubling – trend is creating the need to change the emergency preparedness playbook.

Cyber criminals are copying the way traditional scammers

follow storms and get vulnerable people to pay cash for cleanup, only to abscond with the money and doing no real work.

Cyber criminals have begun to follow natural disasters too, but their targets are often water and power supply operations, hospitals and other critical operations – hitting them with cyber ransom attacks when they are most vulnerable.

Unlike the hackers of old, these bad guys aren't necessarily after a data heist. Hackers today want to highjack an online system and hold it hostage until a hefty – often six- or seven-figure – ransom is paid. Ransom attacks have increased 400% this year over last year, and a whopping 800% since the onset of the pandemic, according to the FBI.

And the price to get untangled from these attacks is escalating as fast. A ransomware attack on Baltimore in 2019, for example, cost the city $18.2 million.

The ransomware threat is so concerning, the Indiana National Guard has tapped Indianapolis-based cyber security firm Pondurance to help conduct disaster drills that layer on cyber threats.

"We're seeing more initiative by these bad actors to exploit these opportunities," says Ron Pelletier, founder and chief customer officer at Pondurance.

"They come in while people and entities are already under duress and distracted," adds Pelletier, an appointed member of the Indiana Executive Council on Cybersecurity (IECC). "It happened recently during the freezing conditions in Texas and created some real havoc. It's becoming more and more prevalent as bad actors become more enterprising. We have to take steps to be prepared."

The IECC was created in 2016 by then Governor Mike Pence to do just that. Governor Eric Holcomb moved to continue the IECC in 2018.

Many of the efforts to bolster Indiana's cybersecurity started

in early 2015, says Chetrice Mosley-Romero, cybersecurity program director at the Indiana Office of Technology and Indiana Department of Homeland Security. “It dawned on state officials that in a real, true cybersecurity emergency we will need a collaborative approach across agencies and organizations.”

Since the IECC’s creation, Indiana’s position in the world of cybersecurity has changed dramatically. It’s essentially gone from one of the worst U.S. states in terms of cybersecurity preparedness to one of the best.

While pleased with this turn of events, Mosley-Romero remains humble. She knows that blowing the trumpet too loudly on the state’s fortification could make it a target for hackers looking to prove their chops.

Mosley-Romero can keep her trumpet put away. The National Governors Association is taking care of that. The organization recently rated Indiana as one of the top five U.S. states in terms of cybersecurity preparedness. That’s quite a change from where the state was just a few years ago.

That ranking, Mosley-Romero explains, is “due to our collaboration, and the fact that we rely on our partnerships for implementation. We were at the bottom before we had the IECC. The things we’ve done at a policy level and with some of our private sector partners is what’s led to our success going from the bottom tier to the top.”

The IECC not only brought on Pondurance, which is doing its part for free, it’s also enlisted the likes of Citizens Energy Group and IU Health among others. The IECC is also reaching out to work with as many local municipalities around the state as possible. “We’re trying to demystify cybersecurity,” Mosley-Romero says. “We have to make this comprehendible to local communities. We have to connect this to something they care about. By doing that, we can get to baselines across counties.”

This comprehensive approach means “we’re not just hitting the breadth of cybersecurity; we’re hitting the depth too. We have the most comprehensive approach of any other state,

and we didn't have that before the formation of the IECC."

Part of that comprehensive approach is training drills.

Officials for the state and the Indiana National Guard hosted two cyber exercises last month in partnership with several federal agencies, health care providers, technology companies, water utility service providers, local government officials, and state and federal emergency and law enforcement agencies.

Pelletier hopes disaster drills, such as these two will raise awareness among policy makers to help fund security programs and protocols.

"National, state and community security is truly at risk here, and we need to take action now to preserve it," he states. "Waiting for the dam to burst before you repair it is a terrible maintenance strategy, and that's exactly the situation we have here across power grids, water supplies, healthcare, you name it."

The first drill was a "tabletop" or virtual exercise that simulated a cyberattack on water system during the July 4 weekend. Holidays are a common time for cybercriminals to hit.

Following the tabletop exercise, a full-scale functional exercise was hosted by the Indiana National Guard for first responders and several military branches as well as search and rescue teams at the Muscatatuck Urban Training Center in southern Indiana.

More than 500 soldiers, airmen and civilian emergency responders from across the state for three days exercised Indiana's response to a catastrophic earthquake and the ensuing chaos, including cyberattacks.

"When natural disasters hit all parts of the world, we are seeing more and more targeted cyberattacks in those affected areas," Pelletier says. "Investing now in preventative measures is the best way to avoid situations like that from becoming worse."

The drills, while perhaps the most visible of what the IECC is involved in, are just the tip of the iceberg. The organization has 121 objectives and 69 deliverables, and has completed 80% of those, Mosley-Romero says.

The state's overall cybersecurity approach is so unique, Mosley-Romero says she fields a constant stream of calls from other states wanting to hear what Indiana is doing for cybersecurity preparedness. "I've talked to dozens of states," she says.

Mosley-Romero stresses that the state isn't holding anything back.

"Our approach to working with other states is like our approach to working with cities and towns across Indiana," she says. "We're all connected, and you're only as strong as your weakest link. The more we collaborate, the better for everyone."

*Adam H. Berry is vice president of economic development and technology at the Indiana Chamber of Commerce. He joined the organization in 2019.*



# Muscatatuck Urban Training Center
# Homeland Defender Info Sheet

INDIANA NATIONAL GUARD

# Homeland Defender 2021

**Exercise Director:** LTC Robert Brake (INNG)

**Executive Council:** Chief Tom Neal (IN TF1) & LTC Robert Brake (INNG)

**Safety Director:** CSM Ty Benham (INNG)

**Operations Director:** Chief Jay Settergren (IN-TF1)

**Operational Support:** CPT Pemberton (INNG)

**MSEL Directors:** DC Steve Coover (MFD & IN-TF1) & LTC Robert Brake (INNG)

UNCLASSIFIED

INDIANA NATIONAL GUARD

# HOMELAND DEFENDER 2021

POC: LTC Rob Brake

## Exercise Mission

INNG host a Full Scale Exercise from 13-15AUG21 vic MUTC involving local and state resources in order to (IOT) reinforce existing relationships, create new ones and share best practices within the 1st responder community.

## Exercise Purpose

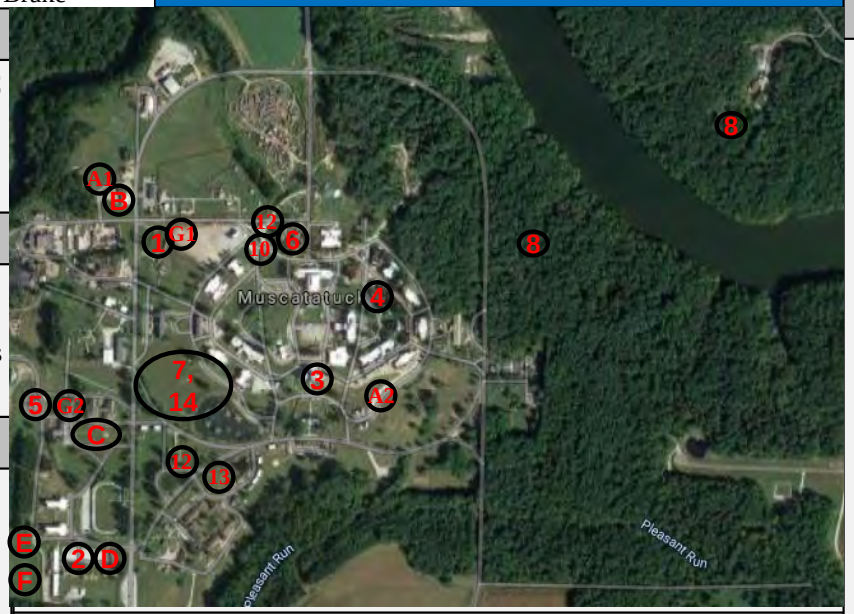
Conduct a joint training event that includes local, state & military partners, focused at the Team level, in order to increase unit/team proficiencies and integration with other 1st responders within the State of Indiana Response Forces.

## Exercise Intent

**Exercise Commander Intent:** Provide a realistic training opportunity for units to collectively train together IOT increase readiness and share tactics, techniques, and procedures via a scalable and nested exercise over a 2 day, weekend exercise. Once completed units, can receive a facilitated AAR based on individual unit training requirements.

**Key Tasks:** Alert & Mobilize, Deploy, Site Occupation, Joint /combined Operations & Redeploy all IAW NIMS.

**End State:** Create a realistic collective exercise from H-hour – OP3, that supports Local and State Inter Agency Integration followed by after action reviews IOT ensure State Partners meet individual and team training objectives, increase readiness and share techniques between Agencies.




## Concept of Operation

A series of earthquakes occur that quickly exceeds local resources requiring assistance from Regional and State Agencies in order to meet lifesaving operational requirements.

As a result multiple agencies and units receive an Alert Orders to Deploy to staging locations. O/O units will move forward IOT conduct Site Occupation & link up with the Incident Management Team (IMT) IOT receive missions for Full Scale Operations. Once units are Mission Complete, they will begin recovery operations and redeploy to home station.

## Operational Lanes:

Lane #1: Initial Command Post & Rail Yard
Lane #2: Unified Command / IMT CMD Post
Lane #3: Hospital Chemical & Radiation
Lane #4: Round Robin Skills Training
Lane #5: Cafeteria Collapse
Lane #6: School Collapse
Lane #7: TF1 Air Load Operations
Lane #8: Lost Personnel WAS
Lane #9: CYBER Ransom
Lane #10: Chaplain Teams
Lane #11: NGRF Alert and Staging Operations
Lane #12: Area Security Operations
Lane #13: Crowd Control Activities
Lane #14: Lifeline Operations

Site A: Staging (Sites 1 & 2)
Site B: MFD & CST CMD Post
Site C: CERFP & TF1 CMD Post
Site D: NGRF CMD Post
Site E: White Cell Team
Site F: Ravenswood Support site
Site G: DECON Sites ( 1& 2)

## Participants/Enablers: 369 (82) BOG -501

CST – 20 (2)
TF1 IN – 6 (15)
CERFP – 208 (5)
CAP – 2
NGRF – 40 (5)
38th CAB – (4)
Ravenswood – (24)
IDHS Dist 8 IMT – 12
127th CB – (2)

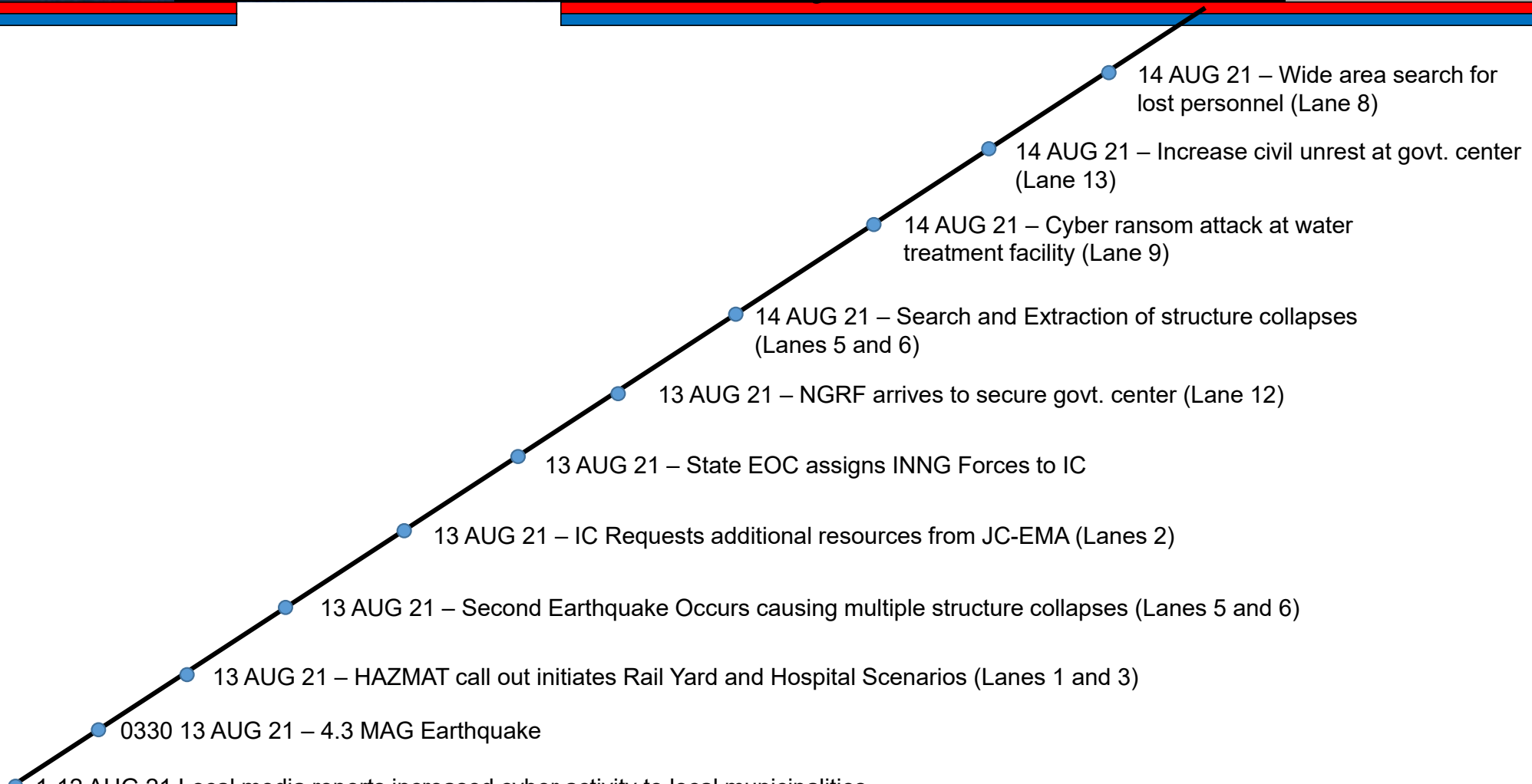
MFD – 16 (6)
81st TC – (10)
IOT – 15 (3)
JCSD – 40
UPAD – 6 (2)
ASOS – 4
JFHQ-IN – (4 )

( ) = non-participant / support role

Additional:
Role Players – (50)

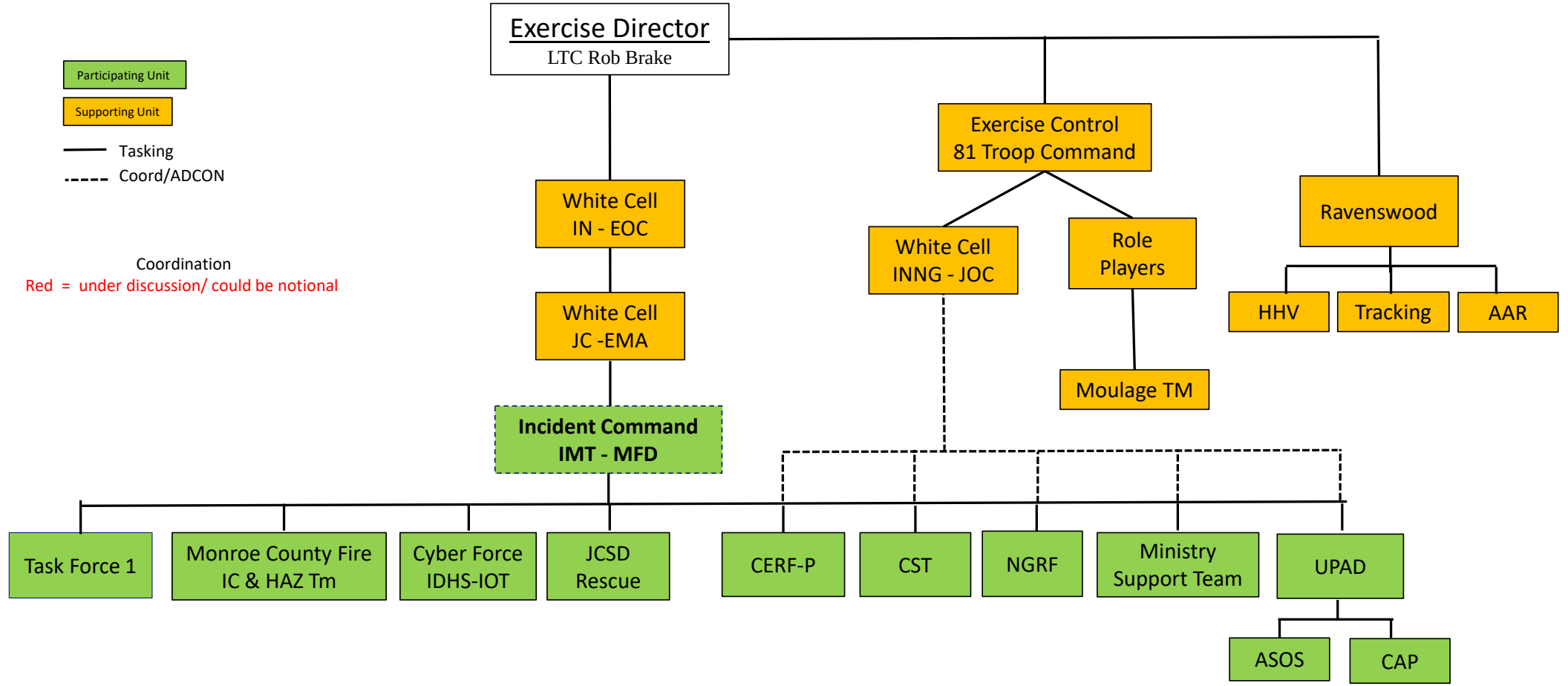
IPR #1 10SEP20 → **CDC** 06-08OCT20 CAIN/MUTC → IPR #2 1NOV20 → IPR #3 4DEC20 → **IPC** 2-3MAR21 MS Teams → **MPC** 16-17MAR21 MUTC → **FPC** 11-12MAY21 MUTC → IPR #4 21JUN21 → IPR #5 19JUL21 → **Execution** 13-15AUG21 MUTC

# Homeland Defender Key Events Timeline



INDIANA NATIONAL GUARD

# Task ORG



# Indiana Emergency Manager Cybersecurity Toolkit 2.0

# INDIANA EMERGENCY MANAGER CYBERSECURITY TOOLKIT


October 2019

*Developed by the Indiana Executive Council on Cybersecurity*

# TABLE OF CONTENTS

Instructions: Please click on the section of the toolkit you would like to skip to in this digital packet.



For more information, visit www.in.gov/cyber.

October 23, 2020

Dear Emergency Managers,

To help our communities continue to be strong and protected while staying connected, Governor Eric J. Holcomb's Executive Council on Cybersecurity has developed this *Indiana Emergency Manager Cybersecurity Toolkit* for local government emergency managers to use as they navigate through the complexities of cybersecurity at a local level.

With October being National Cybersecurity Awareness Month, it is the perfect time for Indiana to launch the first-of-its-kind toolkit you can start using today. As emergency managers we need to convey the importance of this pervasive and serious threat to the many partners in our communities we already coordinate with every day on other threats and hazards. This ever-growing threat is becoming more and more of a concern as many of our own local governments in Indiana have been attacked in the last several months. The best way to approach this new threat environment is like all others: we assess, we plan, we train, and we exercise to best be prepared when a cyberattack happens.

I am looking forward to your input on this cybersecurity toolkit that is meant to be a resource for emergency managers throughout the state. Your feedback will help as we seek to improve it over the coming months.

I hope this also provides the necessary information and tools to get you started so your community is better equipped to prepare and plan for a threat that is increasing by the day with your leadership, peers, and community partners.

Sincerely,

Stephen Cox

Indiana Department of Homeland Security Executive Director &

Indiana Executive Council on Cybersecurity Chair

# HOW TO USE THIS TOOLKIT

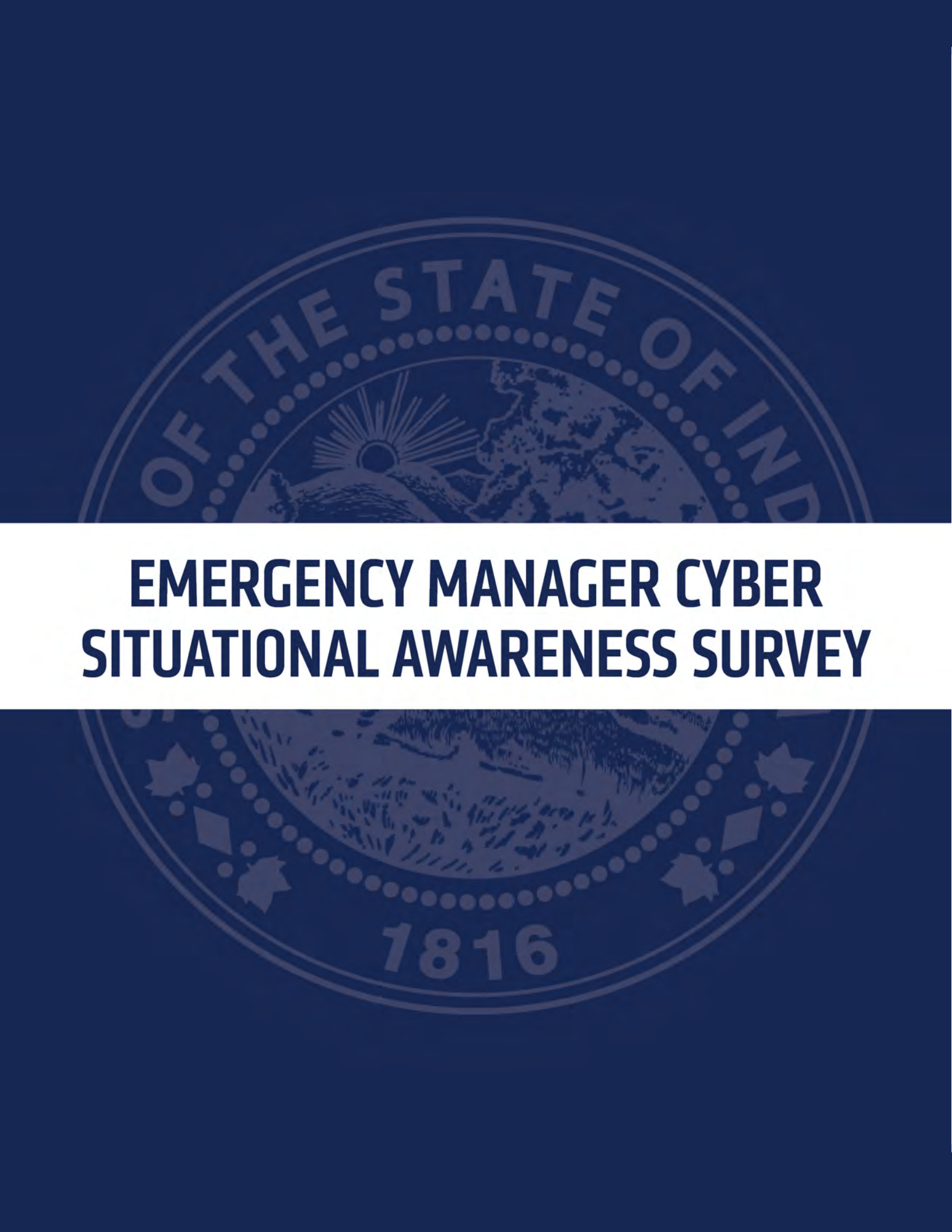
# HOW TO USE THIS TOOLKIT

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 *Indiana Emergency Manager Cybersecurity Toolkit*, developed by the Indiana Executive Council on Cybersecurity, outlines a way to begin conversations with your local partners as simply and directly as the complexity of the effort allows.

This toolkit is primarily for emergency managers who serve their local communities and is organized into four main sections: a survey to assist emergency managers in planning with partners they work with to develop emergency and continuity of operations plans; a cybersecurity incident response plan template; a training and exercise guide; and several additional resources to assist in navigating this new and pervasive threat.

The toolkit can be used holistically or piece-by-piece, depending on how deep you want to go with your planning what you would do if your organizations experience a cyber attack.

This toolkit and additional information for emergency managers can also be found at www.in.gov/cybersecurity/3818.htm.




# EMERGENCY MANAGER CYBER SITUATIONAL AWARENESS SURVEY

# EMERGENCY MANAGER CYBER SITUATIONAL AWARENESS SURVEY

## INSTRUCTIONS

Below are instructions for the Emergency Manager Cyber Situational Awareness Survey. This survey was made to assist local government emergency managers who want to better assess the areas within their purview while developing and exercising their cyber emergency incident response and continuity of operations plans. This Emergency Manager Cyber Situational Awareness Survey was developed by the Indiana Executive Council on Cybersecurity, National Governors Association Cybersecurity Academy participants, as well as Indiana State University. This survey is meant to begin conversations between an emergency manager and his/her local government partners as well as provide a collective overview of the emergency manager's area through a risk profile using the information provided.

Using this survey and working with the Cybersecurity Program Director from the Indiana Department of Homeland Security and Indiana Office of Technology, an emergency manager will be provided with a comprehensive risk profile provided by the State of Indiana in partnership with Indiana State University so an emergency manager is better informed as to what he or she should be focusing on when planning for a cyber attack. All information provided to the state will be kept confidential.

Emergency Manager Cyber Situational Awareness Survey Instructions:

1. The Emergency Manager, who is the main point of contact for the state, retrieves the Emergency Manager Cyber Situational Awareness Survey PDF file online at https://www.in.gov/cybersecurity/3818.htm.
2. The Emergency Manager completes the "Emergency Management Overview" (EMO) page to document the critical infrastructure (CI) and key resource systems within their oversight.
3. Using the critical infrastructure and key resource systems identified in the EMO as a point of reference, the Emergency Manager communicates with a point of contact who is responsible for each individual CI and key resource system(s) identified, and requests they complete the survey for their area.
4. Those responsible for the CI and key resource systems complete his or her copy of the Cyber Situational Awareness Survey (CSAS). The survey can be done on the fillable PDF or completed by hand.
5. Those responsible for the CI and key resource systems send their completed survey back to the Emergency Manager.

6. Once the EMA collects all the completed surveys, he or she will send their overview survey sheet and all the surveys completed (saved or scanned) to the State of Indiana Cybersecurity Program Director Chetrice Mosley at MosleyCLM@iot.in.gov.
7. The State of Indiana, working with a secure lab at Indiana State University, will then complete an analysis and develop a custom confidential Risk Profile for each Emergency Manager.
8. The Risk Profile will then be provided to each Emergency Manager allowing them to: better inform their planning, heighten training, and create appropriate exercises for their areas of responsibility. Emergency Managers will then communicate to their leadership the current status of their cybersecurity posture and priorities.

If you have any questions, please feel free to email the State of Indiana Cybersecurity Program Director Chetrice Mosley at MosleyCLM@iot.in.gov or call her at 317-607-3178.

# Emergency Manager Cyber Situational Awareness Survey

| | |
|---|---|
| Name of County: | Name of City: |
| Address: | |
| Phone: | IDHS District: |
| Email Address: | Population of area supervised: |

**What critical infrastructure and key resource systems do you oversee as an emergency manager in your organization? Select all that apply.**

| |
|---|
| **Communications** |
| County or Municipality Owned Telecommunication Services (Cable, Broadband, etc.) |
| **Dams** |
| **Educational Facilities (K-12 School Systems)** |

| | |
|---|---|
| **Emergency Services** | |
| | Law Enforcement |
| | 9-1-1 Operations |
| | Emergency Management |
| | Fire & Rescue |
| | Emergency Medical Services |
| **Energy** | |
| | County or Municipality – Ran Electricity |
| | County or Municipality – Owned Oil |
| | County or Municipality – Owned Natural Gas |
| **Elections** | |

| | |
|---|---|
| **Government Facilities** | |
| | Offices and Office Building Complexes |
| | Housing for Government Employees |
| | Correctional Facilities |
| | Embassies, Consulates, and Border Facilities |
| | Courthouses |
| | Libraries and Archives |
| **Healthcare & Public Health** | |
| | Public Health Departments |
| | County or Municipality Owned Hospitals or Health Facility |

| **Political Offices** |
| --- |
| Auditor |
| Assessor |
| County Commissioner |
| Sheriff |
| **Transportation Systems** |
| Aviation |
| Highway & Motor Carrier |
| Maritime Transportation Systems |
| Mass Transit & Passenger Rail |
| Pipeline Systems |
| Freight Rail |
| Postal & Shipping |

| |
|---|
| ☐ **Wastewater – Publicly owned wastewater treatment systems** |
| ☐ **Water – Public drinking water systems** |
| ☐ **Other:_____** |

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

| Organization Name: | Name of Person Completing Survey: |
|---|---|
| Address: | |
| Phone: | Email: |

## *Organization Information*

1. How many employees are there in your organization? _____
2. How many employees have information/technology related duties? _____
3. How many employees have cybersecurity related duties? _____
4. How many times in the last 5 years has your organization been the victim of a cyberattack? _____

| | Yes | No |
|---|---|---|
| 5. Do you have cybersecurity policies? | | |
| 6. Do you outsource your cybersecurity needs? | | |
| 7. Do you include security requirements in your agreements with vendors? | | |
| 8. Has your organization completed a cyber assessment in the last 2 years? | | |

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Voice Communications*

**9**. What voice communication systems does your organization use? Select all that apply.

Voice Over Internet Protocol (VOIP) Telephones or Services:

Uses voice over Internet Protocol (IP) technologies for placing and transmitting telephone calls over an IP network, such as the Internet, instead of the traditional public switched telephone network (PSTN) with an analog phone.

Analog Telephones (POTS):

Voice-grade telephone service employing analog signal transmission over copper loops, aka plain old telephone service or plain ordinary telephone service.

Digital Handheld Radios:

Person-to-person two-way radio voice communications systems which use portable, mobile, base station, and dispatch console radios. These systems are used by police, fire, ambulance, and emergency services, and by commercial firms such as taxis and delivery services.

Digital Console Radios:

Same as above description but in non-mobile form.

Satellite Telephones:

Type of mobile phone that connects to other phones or the telephone network by radio through orbiting satellites instead of terrestrial cell sites, as cellphones do.

Radio over Internet Protocol (RoIP):

Like Voice over Internet Protocol (VoIP), but augments two-way radio communications rather than telephone calls.

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Voice Communications (cont.)*

☐ Employer-Issued Cellular Smartphone (e.g. iPhone, Android):
Smartphone owned, issued, supported, and paid for by the employer, and the employee typically agrees to specific usage guidelines.

☐ Personal Cellular Smartphones (e.g. iPhone, Android):
Smartphone that is owned, supported, and paid for by an individual.

☐ Other: _____

## *Data Communications*

**10**. What data communication systems does your organization use? Select all that apply.

☐ Government Email (.gov):
The .gov top-level domain (TLD) facilitates collaboration among government-to-government, government-to-business, and government-to-citizen entities.

☐ Commercial Email (.com/.net) (e.g. Gmail, Yahoo, iCloud):
Free web-based email service (webmail) providers. Typically accessed via web browser or smartphone app.

☐ Wireless Local Area Network:
A wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area (WIFI).

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Data Communications (Cont.)*

Organization Provided Internet Service:

Your company, organization, etc… is provided access to the Internet via a 3rd party Internet Service provider (ISP).

Mobile WiFi Hotspots:

An ad hoc wireless access point that is created by a dedicated hardware device or a smartphone feature that shares the phone's cellular data.

Publicly Accessible Website:

A collection of related network web resources, such as web pages, multimedia content, which are typically identified with a common domain name, and published on at least one web server. Notable examples are wikipedia.org, google.com, and amazon.com.

Organization Email (.com/.org):

A business email address / service given to an employee by the company where they work.

Wired Local Area Network:

A computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

Commercial Internet Service (Xfinity, Comcast, Spectrum):

An organization that provides services for accessing, using, or participating in the Internet.

Government Provided Internet Service:

Your company, organization, etc… is provided access to the Internet via a Government Internet Service provider, ex: Local, County, City, State of Indiana, or Federal.

Internal Network / Website (Intranet):

A computer network for sharing corporate information, collaboration tools, operational systems, and other computing services only within an organization, and to the exclusion of access by outsiders to the organization.

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Data Communications (Cont.)*

Restricted Website (e.g. anything that uses HTTPS):

A controlled private network that allows access to partners, vendors and suppliers or an authorized set of customers – normally to a subset of the information accessible from an organization's intranet.

Other: _____

## *Data Types*

**11**. What data types does your organization use? Select all that apply.

Sensitive / FOUO Information:

Unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest.

Law Enforcement Sensitive Information:

Denotes information that was compiled for law enforcement purposes and should be afforded security in order to protect certain legitimate Government interests

Protected Critical Infrastructure Information:

Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems.

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Data Types (cont.)*

Vital Public Records:

Records of life events kept under governmental authority, including birth certificates, marriage licenses (or marriage certificates), and death certificates. In some jurisdictions, vital records may also include records of civil unions or domestic partnerships.

Medical Records:

Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage.

Court Records:

The official written documentation of what happened during a trial or a hearing.

Purchasing / Contract Records:

Typical contract types include fixed-price, cost-reimbursement, incentive contracts, time-and-materials, labor-hour contracts, indefinite-delivery contracts, Bilateral, Unilateral, Express, Contract Under Seal, etc.

Credit Card Information:

Includes: Primary Account Number (PAN), Cardholder Name, Expiration Date, Service Code, Full track data (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, PINs/PIN blocks.

Bank Account Information:

Includes Social Security number, Online login or password, One Time Password (OTP), Debit or credit card number, ATM card number or PIN, Routing number, Account number, Personal check, Paystub, Driver's license information, Children's personal information.

Personally Identifiable Information (e.g. social security Numbers, bank account numbers, email addresses):

Data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Other: _____

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Data Storage & Equipment*

**12**. Where is your data stored and what equipment is used in organization? Select all that apply.

Organization-Managed Data Center - In-Building:

A dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems.

Organization Data Center – Offsite:

A building, dedicated space within a building, or a group of buildings[4] offsite, used to house computer systems and associated components, such as telecommunications and storage systems

Vendor Managed Data Center – Cloud Based:

A remote version of a data center – located somewhere away from your company's physical premises – that lets you access your data through the internet.

Network Infrastructure (e.g. routers, switches, hubs):

The hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network. It provides the communication path and services between users, processes, applications, services and external networks/the internet.

Desktop Computers:

A personal computer designed for regular use at a single location on or near a desk or table due to its size and power requirements.

Tablets (iPad, Surface):

A mobile device, typically with a mobile operating system and touchscreen display processing circuitry, and a rechargeable battery in a single, thin and flat package

Secured Employee Drives:

A technology that encrypts the data stored on a hard drive using sophisticated mathematical functions

Desktop Printers / Scanners:

Personal printers are primarily designed to support individual users, and may be connected to only a single computer.

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## *Data Storage & Equipment* (cont.)

Networked Printers/Scanners:

Networked or shared printers and/or scanners.

Cellular Telephones:

A portable telephone that can make and receive calls over a radio frequency link while the user is moving within a telephone service area.

Local Servers – In-Office:

A computer program or a device that provides functionality for other programs or devices.

External Hard Drives:

An external hard drive is a portable storage device that can be attached to a computer through a USB or FireWire connection, or wirelessly.

CD-ROM:

A pre-pressed optical compact disc with the capacity to hold approximately 700MB of data.

Networked Shared Drives:

A computer attached to a network that provides a location for shared disk access, i.e. shared storage of computer files (such as text, image, sound, video) that can be accessed by the workstations that are able to reach the computer that shares the access through a computer network.

Thumb Drives:

A USB flash drive -- also known as a USB stick.

Other: _____

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

**13**. On a scale of 1 to 5, with 1 being least confident and 5 being most confident, how confident are you in your accounting for your organizations' voice communications, data communications, data types, and data storage and equipment?

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|

## *Operations Impact*

**14**. On a scale of 1 to 5, with 1 being no impact on your day-to-day operations and 5 being the most impact on your day-to-day operations (e.g. you must close), what level would your organization's operations be affected If taken down by a cyberattack?

| | | | | | |
|---|---|---|---|---|---|
| Operation Systems | ☐1 | ☐2 | ☐3 | ☐4 | ☐5 |
| Voice Communication Systems | ☐1 | ☐2 | ☐3 | ☐4 | ☐5 |
| Email System | ☐1 | ☐2 | ☐3 | ☐4 | ☐5 |
| Databases of Information | ☐1 | ☐2 | ☐3 | ☐4 | ☐5 |

## CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

| *Public Safety and Health Impact* | Yes | No |
|---|---|---|
| **15.** If your operation systems are down/compromised will the health and/or safety of the public be at risk? | | |
| **16.** If your information systems are down/compromised will the health and/or safety of the public be at risk? | | |
| **17.** If your communication systems are down/compromised will the health and/or safety of the public be at risk? | | |
| **18.** If your email system is down/compromised will the health and/or safety of the public be at risk? | | |

| **Preparedness and Response** | | |
|---|---|---|
| **19.** Does your organization have multi-factor authentication? | | |
| **20.** Does your organization install computer updates and/or patches regularly? | | |
| **21.** Do you install your updates and/or patches automatically? | | |
| **22.** Does your organization have a cyber emergency response plan in place to address a cyberattack on your organization? | | |

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

| Preparedness and Response (cont) | Yes | No |
|---|---|---|
| **23.** Does your organization provide your employees cybersecurity awareness and/or training? | | |
| **24.** Does your organization have a continuity of operations plan? | | |
| a) If yes, does your continuity of operations plan account for a cyber attack? | | |
| **25.** Are your organization's 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) periodically monitored and scanned for security vulnerabilities and malicious software? | | |

# CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

## Recovery

**26**. In the event of a critical information system disruption or loss, what backup or redundant systems are in place for your organization?

**System Types**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Operation Systems** | Multiple automatic backup systems are in place | An automatic or manual backup system is in place | A manual backup system is in place | Improvised system backups can be employed | No backup system is in place | I do not know |
| **Email Systems** | Multiple automatic backup systems are in place | An automatic or manual backup system is in place | A manual backup system is in place | Improvised system backups can be employed | No backup system is in place | I do not know |
| **Information from Databases** | Multiple automatic backup systems are in place | An automatic or manual backup system is in place | A manual backup system is in place | Improvised system backups can be employed | No backup system is in place | I do not know |

**27**. On a scale of 1 to 5, with 1 being least confident and 5 being most confident, how confident are you in your preparation, response, and recovery abilities in the event of a cyberattack?

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|


# CYBERSECURITY INCIDENT RESPONSE PLAN TEMPLATE

[NAME OR ORGANIZATION OR ADD LOGO]

[DOCUMENT TITLE]

---

[DOCUMENT SUBTITLE]

ORGANIZATION, DEPARTMENT OR AUTHOR NAME

DATE

CYBERSECURITY INCIDENT RESPONSE PLAN TEMPLATE

DRAFT FOR REVIEW

**Table of Contents**

I. INTRODUCTION

A. PURPOSE

General statement of what the response plan is meant to accomplish. The statement should be supported by a brief synopsis of the plan's contents.

B. SCOPE

States specifically the facilities, groups, departments, units, or personnel to which the plan applies.

C. SITUATION OVERVIEW

1. Describes, in very general terms, the current planning environment and the types of cybersecurity threats the planning organization must be prepared to manage.

2. Types of cybersecurity threats

a) Adverse Impact to Organization. These events have significant impact on the normal operations but do not fall into any of the following categories.

b) Alteration/Compromise of Information. These events involve the unauthorized altering of information or incidents that involve the compromise of information.

c) Denial of Service Attacks. These events are attacks that affect the availability of critical resources such as email servers, web servers, routers, gateways, or communication infrastructure.

d) Loss or Theft. These events involve the potential compromise of sensitive material. This includes the compromise of user accounts and passwords that could allow unauthorized persons to access IT resources.

e) Probes and Scans. These events include probing or scanning networks for critical services or security weaknesses. It also includes nuisance scans.

f) Unauthorized Access and Unsuccessful Attempts. These events include all successful unauthorized accesses and suspicious unsuccessful attempts.

g) Virus/Worms/Malicious Code. These events are performed by hackers in an attempt to gain privileges and/or information, to capture passwords, and to modify audit logs to hide unauthorized activity. The attempts include the use of mobile code such as viruses, Trojan horses, worms,

and scripts. This category includes any virus or code that is intended to disrupt or annoy users.

3. Relative probability and potential impact of threats.

4. Vulnerability of critical systems.

5. Dependency of external organizations, vendors, or government agencies.

6. Current asset identification, hazard prevention, protection, and mitigation measures that are in place.

D. PLANNING ASSUMPTIONS

1. Describes what the planning team assumes to be facts for planning purposes in order to execute the plan.

2. During response operations, the assumptions indicate areas where adjustments to the plan have to be made as the facts of the incident become known.

## II. CONCEPT OF OPERATIONS

A. DETECT

1. Procedures, processes, and systems in place for monitoring and detecting threats and anomalies.

2. Description of how continuous threat monitoring and detection is maintained.

3. Processes in place for evaluating effectiveness of monitoring, detection, and protective measures.

B. RESPOND

1. Threat Notification:

a) Upon detection of an event or threat, describes the process for preliminary alert messaging which communicates the existence of an

emergency situation and provides basic incident information necessary to initiate an effective response.

b) Where will initial notifications originate?

c) Who will receive initial notifications? Establishes initial point of contact for initial incident alerts by position or job title

d) What information is provided in the initial notification?

2. Situation Assessment:

a) Process of gathering initial incident information, establishing situational awareness, determining severity of impacts, assessing needs, and determining whether to activate the incident response operations.

b) Incident triage and analysis process to determine nature, complexity, and severity of incident.

c) Incident response priorities based on existing or anticipated impacts to normal operations. Examples:

(1) Protect human life and safety. Protection of human life always takes precedence over all other considerations.

(2) If applicable, protect classified data as regulated by government statutes and regulations.

(3) Protect sensitive data, including proprietary, financial, law enforcement, scientific, and managerial data.

(4) Prevent system damage (e.g., loss or alteration of system files, damage to hard drives).

(5) Minimize disruption of computing resources. In many cases, it is better to shut down a system or disconnect from a network than to risk damage to data or systems.

d) Thresholds and trigger points for escalating and mobilizing response activity if an incident becomes more critical.

e) Identify and describe the actions that will be taken to monitor the movement and future effects that may result from the emergency.

f) Describe how the initial assessment is disseminated/shared in order to make protective action decisions and establish response priorities.

3. Response Plan Activation

a) Establishes which individuals by position/job title who have the authority to activate the response plan and initiate response operations.

b) Describes response process flow.

c) Details decision-making process for plan activation and initiation of coordinated response activity.

d) Procedures for assembling, and deploying personnel, supplies, and equipment to support the response to an incident.

4. Alert and Warning

a) Processes for reporting threats, events, and anomalies to elected and appointed officials, community leadership, management, personnel, law enforcement, and external stakeholders.

b) Establishes minimum reporting information requirements. (i.e. date, time, name and title of reporting person, location, systems/applications affected, etc.)

c) Identify and describe the actions that will be taken to coordinate, manage, and disseminate notifications effectively to alert/dispatch response and support agencies.

d) Identify and describe the actions that will be taken to notify and coordinate with adjacent jurisdictions.

5. Response Operations

   a) Describes deployment and management of response tasks, personnel, and resources to ensure life safety, stabilize the incident, isolate threat, limit impact, and protect property.

   b) Details how command and control is established (i.e. Incident Command, EOC, etc.)

   c) Development of incident response goals and objectives (i.e. incident action plan)

6. Demobilization

   a) Organized deactivation and release from duty of emergency response resources and personnel.

   b) Describe process of developing demobilization plan.

   c) Identify the individual by role, position, or job title that has the authority to release personnel and resources from duty.

   d) Outline decision-making process for determining when demobilization will take place

   e) Establish criteria for releasing personnel and resources.

7. Incident Close Out and Response Deactivation

   a) Identify processes for collection of required documentation.

   b) Identify processes to manage the accounting of supplies, equipment, and other materials.

   c) Describe formal transition process/change of command from response to recovery operations.

   d) Notification process to internal and external stakeholders of formal end to response operations, transition to recovery operations, and /or return to normal activity.

C. RECOVER

1. Describe process of preserving and restoring critical applications, systems and services in order to resume normal operations.

2. Disaster Recovery

    a) Identify individuals by position/job title that would have operational authority over recovery activity, if different from response phase.

    b) Establish process for implementing the organization's information technology (IT) disaster recovery plan.

3. Business Continuity

    a) Discuss implementation of existing plans to ensure continuity of critical government services and business activity, and expedite resumption of normal operations.

4. System/Application Restoration

    a) Describe procedures to restore systems to the original state and validate the system has been cleared of any detected threats.

    b) Describe how affected and restored systems are tested and validated before being brought back online.

5. After Action Review (AAR) and Improvement Planning

    a) Detail process used by the jurisdiction to review and discuss the response in order to identify strengths and weaknesses in the emergency management and response program.

    b) Describe how the jurisdiction ensures that the deficiencies and recommendations identified in the AAR are corrected/completed.

III. ASSIGNMENT OF RESPONSIBILITIES

A. General list of tasks to be performed, by position and/or department, without the procedural details included in standard operating procedures.

B. Organizational charts can also be inserted here (i.e. Incident Command, Emergency Operations Center, Security Operations Center, Crisis Management Team, etc.)

IV. DIRECTION, CONTROL, AND COORDINATION

A. Identifies the individuals by position/job title that have operational and management authority over response operations.

B. Outlines how response activity and resource management is coordinated internally as well as with external stakeholders, vendors, agencies, and organizations.

V. INFORMATION COLLECTION, ANALYSIS, AND DISSEMINATION

A. Identifies the type of information needed, the source of the information, who uses the information, how the information is shared, the format for providing the information, and any specific times the information is needed.

VI. COMMUNICATIONS

A. Describes the communication protocols and coordination procedures used between response organizations during emergencies and disasters.

VII. ADMINISTRATION, FINANCE, AND LOGISTICS

A. Outlines general support requirements and the availability of services and support for incident response, as well as general policies for managing resources.

B. Describes pre-incident, operational, and post-incident documentation requirements

C. Existing contracts and contracting requirements for material resources, staffing, and vendor-managed services.

D. Purchasing and procurement requirements.

E. Cost tracking and funding requirements.

F. Inventory, supply, and resource tracking.

G. Processes for addressing legal issues and regulatory requirements.

VIII. PLAN DEVELOPMENT AND MAINTENANCE

A. Discusses the overall approach to planning and the assignment of plan development and maintenance responsibilities.

B. Assigns responsibility for the overall planning and coordination to a specific individual by job title within the organization.

C. Establishes process and schedule for plan development, review, training, exercise, evaluation, and improvement.

IX. POLICIES, AUTHORITIES, AND REFERENCES

A. Lists of laws, statutes, ordinances, executive orders, regulations, and formal agreements relevant to emergencies.

B. Specifies the extent and limits of the emergency authorities granted to the senior official, including the conditions under which these authorities become effective and when they would be terminated

C. Identifies state, national, international, and professional standards that apply to the plan.

D. Establishes any pre-delegation of emergency authorities that may not be described in other planning documents.


# CYBERSECURITY TRAINING AND EXERCISE GUIDE

# CYBERSECURITY TRAINING AND EXERCISE GUIDE

## Table of Contents

# I. Introduction

## A. Purpose

As part of an all-hazards approach to emergency management, the *Cybersecurity Training and Exercise Guide* provides general information and instructions for establishing and implementing an effective cybersecurity training and exercise program.

The contents of this Guide are intended to align state and federal emergency management training and exercise requirements with cybersecurity training and education standards established by the National Institute of Standards and Technology (NIST). In addition to NIST, this Guide incorporates concepts and elements from the Homeland Security Exercise and Evaluation Program (HSEEP), National Incident Management System (NIMS), Emergency Management Accreditation Program (EMAP), and National Fire Protection Association (NFPA).

## B. Scope

The Guide is intended for emergency managers in municipal, county, and local government agencies. It may also be useful to individuals responsible for emergency preparedness and business continuity functions in other public sector, private sector, healthcare, and academic organizations.

There are a wide variety of potential cyber threats and a constantly evolving list of methods and tactics used to conduct cyberattacks. The training and exercise activity outlined here is focused on cyber incidents that may:

-Pose an immediate threat to public health, safety, and security;
-Impact or disrupt the delivery of essential government and social services; or
-Require a coordinated, multi-agency, multi-disciplinary response

## C. Situation

Cybersecurity incidents and cyberattacks on computers, information networks, and communications systems are now part of the complex threat environment emergency managers must face.

In the State of Indiana, numerous high-profile cyberattacks have occurred in recent years. Targets of these attacks included government agencies, healthcare facilities, community organizations, businesses, school systems, and universities. Attacks have occurred in every region of the state and affected communities and organizations large and small, rural and urban.

Most of these incidents have involved the theft of sensitive data or ransomware attacks. These incidents had significant financial and public relations impacts, but did not pose an immediate safety threat. However, cyberattacks are increasingly targeting critical infrastructure sectors. A successful cyberattack on critical infrastructure could cause real-world operational damage and trigger cascading impacts that threaten public safety.

Nationally, in the vast majority of cybersecurity incidents, it was a lack of awareness and coordination that allowed the attacks to occur and delayed the response to the incidents. The problem was a failure to train and educate all people who are access points to information and operations systems, not a failure of technology or lack of resources.

Collaborating with information technology (IT) professionals and integrating cybersecurity training into a comprehensive emergency management program can help reduce the risk of a cyberattack, improve incident response, and limit the impacts should an attack occur.

This Guide is being used to address training gaps identified in a formal cybersecurity risk assessment and/or incident response planning process.

### D. Assumptions

In developing this document, it was assumed the government entity or organization intending to use the Guide had the following measures and practices in place:

- The Guide is being used to address training gaps identified in a formal cybersecurity risk assessment and/or incident response planning process.
- An individual, group, department, agency or third-party vendor is assigned and is responsible for managing information technology resources and information security for the government agency or organization.
- There are established organizational rules and policies in place for the safe and secure use of computers, tablets, mobile devices, personal devices, and any other internet-capable electronic devices issued to or used by an employee.
- Employees are made aware of device usage rules and IT incident reporting procedures.
- The user of this Guide is familiar with the concepts and practices outlined in the Homeland Security Exercise and Evaluation Program (HSEEP).
- Emergency managers have a basic awareness of cybersecurity threats and intend to include information technology professionals in cyber incident response planning, training and exercise activity.

## II. Training

Training is essential for protecting information and operation network systems and effectively responding to a cybersecurity incident. Training recommendations and suggested online, classroom, and resident training courses for emergency managers, IT professionals, and cybersecurity stakeholders are included in this section.

These courses can provide a basic understanding and awareness for both cybersecurity and emergency management concepts. The goals are for emergency managers and IT professionals to “speak each other’s language” and promote joint planning, training, and exercise activity.

### A. Essential Cybersecurity Awareness Training for All Users

People in an organization are both the greatest vulnerability and best line of defense in regard to cybersecurity. Training can be delivered as part of formal or ad hoc new employee training, ongoing in-service training, or as-needed at the direction of IT managers, supervisors, or executives.

Recommended best practices for cyber hygiene and critical information security training content are outlined in this section. Additional cybersecurity training can be found on Indiana's Cybersecurity Hub at www.in.gov/cybersecurity/3811.htm.

1. Basic Device and System Usage: Training that provides all users of an organization's information technology resources, including staff, managers, executives, and contract employees, awareness of policies and rules regarding the acceptable use of information devices and systems. This could include:
    - Mobile telephone, device, and application use
    - Computer use and portable data storage
    - Access to data networks, servers, drives, and folders
    - Internet browsing and social media restrictions
    - Approved use of official email and messaging applications
    - Personal mobile device and computer use for official business
2. Information Security Awareness: Instruction regarding the need and importance of information security, privacy measures, and cyber hygiene within an organization to protect valuable data, devices, and network systems. Examples include:
    - Physical security and protective measures for computers and mobile devices
    - Use of strong passwords for computers, mobile devices, email, and network access
    - Secure use of external data storage devices such as flash drives and external hard drives
    - Employee role in maintaining and supporting routine software updates, antivirus software, and firewall protections
    - Requirements for remote network access and use of virtual private networks
    - Use of public, personal, or unsecured Wi-Fi networks
    - Cyberattack methods, vectors, and tactics
    - Recognizing social engineering attempts, phishing emails, and malicious websites
    - Awareness of cybersecurity threats to mobile devices including location services, USB charging devices, mobile apps, malicious QR codes and texts messages

3. Incident Response Procedures: Internal processes and procedures for reporting and initially responding to unexplained computer or system malfunctions, unusual or suspicious network activity, loss of data or data access, detection of malicious software, or a confirmed cyberattack. Information provided in training could include:

    - Primary and alternate points of contact and methods for reporting a suspected or confirmed cybersecurity incident.
    - Essential information to provide when reporting an incident.
    - Immediate actions the user must take to help contain a suspected or confirmed cybersecurity threat.
    - The user's role in supporting an incident response including analysis, containment, eradication, evidence gathering, and recovery.

## B. Cybersecurity Training for Emergency Managers

These course recommendations are intended to familiarize emergency managers with cybersecurity terminology, core concepts, and best practices.

Training providers include the FEMA Emergency Management Institute (EMI), Texas A&M Engineering Extension Service (TEEX), Norwich University (NUARI), University of Texas San Antonio (UTSA), and the Criminal Justice Institute (CJI).

Detailed course information is available in the FEMA National Preparedness Course Catalog.

Basic

AWR-136: Essentials of Community Cyber Security (TEEX, Classroom)

AWR-175-W: Information Security for Everyone (TEEX, Online)

AWR-176-W: Disaster Recovery for Information Systems (TEEX, Online)

Intermediate

AWR-169-W: Cyber Incident Analysis and Response (TEEX, Online)

AWR-177-W: Information Risk Management (TEEX, Online)

AWR-366-W: Developing a Cyber Security Annex for Incident Response (NUARI, Online)

IS0523: Resilient Accord: Exercising Continuity Plans for Cyber Incidents (EMI, Online)

E0553: Resilient Accord: Cyber Security Planning Workshop (EMI, Classroom)

Advanced

AWR-353-W: Using the Community Cyber Security Maturity Model (UTSA, Online)

MGT-384: Community Preparedness for Cyber Incidents (TEEX, Classroom)

MGT-385: Community Cyber Security Exercise Planning (TEEX, Classroom)

MGT-452: Physical & Cybersecurity for Critical Infrastructure (TEEX, Classroom)

MGT-456: Integration of Cybersecurity Personnel into the EOC for Cyber Incidents (NUARI/TEEX, Classroom)

## C. Emergency Management Training for IT Professionals

These course recommendations are intended to provide IT professionals and cybersecurity stakeholders with foundational knowledge of emergency management. This includes Incident Command System, NIMS, emergency operations centers, exercise planning, and how IT professionals can be integrated into a coordinated response to a major cybersecurity incident.

Basic

IS0908: Emergency Management for Senior Officials (EMI, Online)

IS0100.c: ICS 100 Introduction to the Incident Command System (EMI, Online)

IS0200.c: ICS 200 Basic Incident Command for Initial Response (EMI, Online)

IS0700.b: National Incident Management System (EMI, Online)

IS0235.c: Emergency Planning (EMI, Online)

Intermediate

IS0546.a: Continuity of Operations Awareness (EMI, Online)

IS0120.c: An Introduction to Exercise (EMI, Online)

IS0775: Emergency Operations Center Management and Operations (EMI, Online)

AWR-366-W: Developing a Cyber Security Annex for Incident Response (NUARI, Online)

IS0523: Resilient Accord: Exercising Continuity Plans for Cyber Incidents (EMI, Online)

Advanced

MGT-456: Integration of Cybersecurity Personnel into the EOC for Cyber Incidents (NUARI/TEEX, Classroom)

E0553: Resilient Accord: Cyber Security Planning Workshop (EMI, Classroom)

PER-257: Cyberterrorism First Responder (UTSA, Classroom)

PER-371: Cybersecurity Incident Response for IT Personnel (CJI, Classroom)

E8515: Cybersecurity Symposium (EMI, Resident Course)

# III. Exercise

Cybersecurity incidents are complex. The response to these incidents is often equally complex, involving groups which are not traditional disaster response or emergency support function partners. Conducting exercises with IT professionals, private sector representatives, and community stakeholders is critical to ensure an effective, coordinated response to a cyberattack.

The nature of cybersecurity threats makes them unique. However, conducting exercises to test and evaluate response capabilities can be accomplished using well-established practices familiar to emergency managers. This section will provide best practices, planning considerations, and suggestions drawn from HSEEP to plan and conduct cybersecurity exercises.

## A. Exercise Planning

1. Exercise Participants: Those taking part in an exercise will vary depending on the nature, scope, and scale of the exercise being planned. This will likely include both traditional and non-traditional partners. Participants to consider could include:

    a) Emergency Support Function (ESF) organizations

    b) Chief Information Officer/IT Director for jurisdiction or organization

    c) IT /Data/Cybersecurity contractor for jurisdiction or organization

    d) Attorney or general counsel for jurisdiction or organization

    e) County Commissioners/County Council Members

    f) Municipally-elected officials/Mayors/Town Manger

    g) City/Town Council members

    h) Auditor, Treasurer, Assessor, Recorder, Surveyor

    i) Prosecutor, Clerk/Clerk of Courts

    j) Township Trustees or designee

    k) Human resources/Personnel department for jurisdiction or organization

    l) Electric power utility or electric cooperative

    m) Water/Wastewater/Stormwater utilities

    n) Natural gas utility

    o) Telecommunications provider or telephone cooperative

p) Hospitals, healthcare facilities, and providers

q) School district representatives

r) Cooperative extension service program representative

s) Chamber of Commerce/Local economic development stakeholders

t) Zoning/Building/Area planning commission members

u) Americans with Disabilities Act/Accessibility Office representative

v) Mass transit/rural transit service providers

w) Vendor-managed and contract service representatives

x) County insurance coverage provider

2. Exercise Planning Team: The composition of the Exercise Planning Team should reflect the agencies, groups, and organizations participating in the exercise. Incorporating subject-matter experts involved in incident planning, response, and recovery will help ensure the exercise scenarios are realistic, challenging, and adequately test key response functions.

   a) Planning Meetings: The complex nature of cybersecurity exercise design and development requires well organized meetings to ensure exercise success. In some situations, participants may be unfamiliar with exercise planning methodology and may never have taken part in a disaster exercise.

   b) Concept and Objectives Meeting: Identify the type, scope, objectives, and purpose.

   c) Initial Planning Meeting: Lay the foundation for exercise development.

   d) Midterm Planning Meeting: A forum for discussing organization, staffing concepts, and exercise logistics.

   e) Master Scenario Events List (MSEL) Meeting: A forum for creating and reviewing the scenario injects and timeline.

   f) Final Planning Meeting: Forum for reviewing exercise logistics, processes, and procedures.

   g) After-Action Meeting: Feedback for participating jurisdictions on their performance and plans for improvement.

3. Documentation: The requirement for exercise documentation will vary depending on the type and size of exercise being conducted, as well as the number and variety of participants.

**Seminar, Workshop, or Game:**

a) Budget

b) Required pre-exercise meeting sign-ins and agendas

c) Presentations (if applicable)

d) Agenda for exercise event

e) Exercise participant rosters/sign-in sheets

f) Executive summary

**Tabletop Exercise:**

a) Budget

b) Required pre-exercise meeting sign-ins and agendas

c) Agenda for exercise event

d) Situation manual

e) Exercise evaluation guides

f) Exercise participant rosters/sign-in sheets

g) After action report/improvement plan

**Drill, Functional, and Full-Scale Exercise:**

a) Budget

b) Required pre-exercise meeting sign-ins and agendas

c) Agenda for exercise event

d) Exercise plan

e) Master scenario events list

f) Controller and evaluator handbook

g) Exercise evaluation guides

h) Exercise participant rosters/sign-in sheets

i) After action report/improvement plan

## B. Special Considerations

Private-sector organizations and critical infrastructure stakeholders may require additional documentation before and after an exercise. There may be legal, regulatory, or internal policy compliance documentation requirements.

These may include memorandums of understanding, sector-specific reporting forms, or non-disclosure agreements.

## C. Discussion-Based Exercises

- Seminars: Orient participants or provide an overview of plans, policies, and procedures. Example: Review of Cybersecurity Incident Response Plan with cybersecurity stakeholders, emergency responders, or elected/appointed officials.
- Workshops: Focus on development of a planning product by the attendees. Example: Develop annexes, standard operating procedures, or checklists to support the activation of an incident response plan. These could be notification checklists, response and containment processes, or recovery procedures.
- Games: Simulation of operations that often involves two or more teams designed to depict an actual or hypothetical situation. Example: Groups of participants test their abilities to recognize and report phishing emails.
- Tabletop Exercise: Guided discussion following an incident scenario used to assess response plans, policies, and procedures. Example: Senior officials, ESF representatives, and IT professional are presented with a series of simulated network system failures and information injects. Participants talk through their coordinated response to a ransomware attack scenario.

## D. Operations-Based Exercises

- Drills: Test of a single operation or function in a single agency or organization. Example: Incident notification procedures and systems are tested to ensure all cyber incident response stakeholders receive alert messages.

- Functional Exercises: Tests individual capabilities, multiple functions, or activities within a function; however movement of personnel and equipment is simulated. Example: Emergency operations center is activated and ESF representatives respond to a simulated cyberattack scenario. Participants manage command, control, and coordination functions in real-time.

- Full-Scale Exercises: Combines command and control elements of a functional exercise with the actual deployment of operational personnel and resources to test incident response capabilities under realistic conditions. Example: IT professionals, public safety officials, and ESF agencies respond to a large-scale cyberattack which impacts critical infrastructure. This would include the deployment of resources and personnel in response to immediate and cascading community impacts of the attack.

## E. Exercise Scenario Ideas

- **Scenario 1**: **Phishing Trip**

  **Target**: Elected and Appointed Officials, System Access Credentials

  **Attack Method**: Spear Phishing

  **Triggering Incident Description**:

  County commissioners, county sheriff's department, and staff members in the county auditor's office receive emails requesting confirmation of their usernames and passwords for their official email accounts. The message says there has been suspicious activity in their email account and their account will be disabled unless they provide the requested information. In some cases, the username and passwords for other systems and databases were requested. The email appears to come from a current county employee with a legitimate email address. Some staff members report providing their username and password information. No system disruptions or suspicious system activity has been observed or reported.

  **Inject Discussion**:

  Who within your organization is notified?

  What is your organization's initial response?

  How do you warn and communicate with employees, contractors, and vendors?

What actions are taken to determine if malware is present or if data has been compromised?

Do you require external agencies or vendor-managed services?

Is law enforcement notified?

- **Scenario 2: The Hacktivist**

  **Target**: Local Government Websites

  **Attack Method**: SQL Injection, Denial of Service

  **Triggering Incident Description**:

  A well-known activist group threatens to shut down local government computer networks on social media. The next morning, multiple agency websites are offline. Some sites are defaced with vulgar, anti-government messages and the insignia of a hacking group. Other sites show error messages or are blank. An initial investigation also shows servers are being overloaded by internet traffic from thousands of sources simultaneously.

  **Inject Discussion**:

  Who within your organization is notified? What is that notification process?

  Are IT disaster recovery and incident response plans in place?

  What is your jurisdiction's initial response to the incident?

  What local, county, and/or state agencies are involved in the response?

  Do you require external or vendor-managed services to restore systems?

  Is law enforcement notified?

  How is public information, social media, and news media messaging managed?

- **Scenario 3: The Break-In**

  **Target**: Financial Data and Personally Identifiable Information

  **Attack Method**: Spyware, Data Extracting Malware

  **Triggering Incident Description**:

  Your jurisdiction is notified by federal and state law enforcement that a large amount of sensitive information from your jurisdiction's databases is being sold on a criminal website. The information included names, social security numbers, addresses, dates of birth, mother's maiden names, checking account, and credit card account information of residents, employees, and contractors. An initial network investigation identified malware that recorded log-in credentials and extracted data from several systems and databases. It is unclear how long the data breach has been in place.

**Inject Discussion**:

What is your organization's initial response?

Who is the lead response agency? Who are the supporting agencies?

Do you require external agencies or vendor-managed services?

How do you identify and warn those affected by the data breach?

Does your jurisdiction have insurance that covers costs related to the breach?

What legal or regulatory issues may result?

- **Scenario 4: The Lockout**

  **Target**: Local Government Computers, Networks, and Data

  **Attack Method**: Ransomware

  **Triggering Incident Description**:

  County employees in multiple local government offices and agencies report being unable to log in to their computers. Those that are able to log in to their computers are unable to access email, public records, and essential databases. Telephones and fax machines are also reported to be offline at several office locations. Fire, law enforcement, and EMS departments have been affected. Public safety communications has been impacted, but computer aided dispatching and 911 telephone systems are still operating normally. A local school system and several municipalities are also reporting similar problems. A message appears on computer screens declaring the computers and systems are locked and will only be released if the hacker is paid $50,000 in bitcoin currency.

  **Inject Discussion**:

  What is your organization's response?

  Are IT disaster recovery and incident response plans in place?

  Are business continuity and continuity of operations plans in place?

  How would your organization communicate internally and externally?

  Does your jurisdiction have cybersecurity insurance?

  Does your jurisdiction have access to bitcoin currency?

  Who is authorized to approve or deny the ransom payment?

  What are the potential cascading impacts to local government and community?

- **Scenario 5: False Alarm**

  **Target**: Outdoor Warning and Mass Notification Systems

**Attack Method**: Spyware, Credential Theft, DMTF Signal Spoofing

**Triggering Incident Description**:

At 11:30 PM, outdoor warning sirens across the county begin to sound. There is no severe weather or local emergency. Sirens were not activated by emergency management or other public safety agency. Attempts to access the siren control system and shut off sirens remotely are unsuccessful. Attempts by emergency management to shut off nearby sirens manually are also unsuccessful. Sirens momentarily deactivate, but immediately reactivate. Public safety dispatchers receive dozens of 911 calls from residents in a matter of minutes. Emergency management also receives reports that text messages falsely reporting a train derailment and hazardous chemical spill are being received on cellphones across the county.

**Inject Discussion**:

What is your organization's response?

What agencies have access to the jurisdiction's outdoor warning and/or emergency mass notification systems?

How can siren and notification system vendors be engaged to assist?

How would you quickly communicate accurate information to the public and media outlets?

What instructions would you provide to the public?

- **Scenario 6: Dispatch Flood**

  **Target**: Public Safety Answering Points

  **Attack Method**: Botnet, Telephony Denial of Service

  **Triggering Incident Description**:

  Public safety dispatchers begin receiving numerous 911 calls which immediately disconnect when answered. Police officers are initially dispatched to the hang-up call locations as the volume of calls grow over several minutes. Nearly 200 calls appear to be originating from the same 20 to 30 mobile telephones in the local area. When arriving on scene, police officers investigating the hang-up calls find residents are unaware of the 911 calls. Upon inspection, the cellphones making the calls appear to be locked with blank screens. Owners are unable to unlock the telephones or power them off. Owners reported that the cellphones "froze" when they clicked on a link in a social media app. similar incidents were reported by public safety agencies in adjacent counties.

  **Inject Discussion**:

  What is your organization's initial response?

  What back-up systems, processes, facilities, or mutual aid agreements are in place?

How would you quickly communicate accurate information to the public and media outlets?

What instructions would you provide to the public?

How would commercial telecommunications and cellular telephone service providers assist? How can vendor assistance be requested?

Is state or federal assistance required? How is assistance requested in this situation?

- **Scenario 7: Flu Season**

  **Target**: Hospital Information Network

  **Attack Method**: Ransomware

  **Triggering Incident Description**:

  It is the height of a very severe flu season. Below zero temperatures and heavy snow are straining local emergency medical services and fire department resources. The emergency department in the community's largest hospital is experiencing a high volume of patients. The hospital is operating at near capacity. The hospital goes on full diversion due to patient volume and reported information network issues. Hospital staff are unable to access the electronic medical records system. The email system also experienced intermittent outages before going completely offline. Facilities staff are unable to access and control heating and ventilation systems. Temperature, air pressure, and humidity in the hospital can no longer be controlled. The system issues are initially blamed on the weather, until a ransomware message appears on multiple computer screens. The message demands $100,000 in bitcoin to restore the hospital's computer systems.

  **Inject Discussion**:

  How would public safety and public health agencies assist?

  Does the hospital have business continuity and emergency operations plans in place?

  What vendor-managed services would be required to maintain safe patient care activity at the hospital?

  Can other hospitals in the area manage the additional patient volume diverted from the affected hospital?

  Does the hospital have cybersecurity insurance?

  Is the hospital willing to pay the ransom?

  At what point would partial or full evacuation of the hospital be required?

- **Scenario 8: From Bad to Worse**

  **Target**: Emergency Management, Emergency Support Functions

  **Attack Method**: Email Extortion, Ransomware, Distributed Denial of Service

  **Triggering Incident Description**:

  A major flood has been impacting large areas of the state for several days and there is widespread damage across the county. The county emergency operations center has been activated to coordinate local response operations. There has been extensive local and national media coverage of the flood and the community's response. Mid-morning on the 5th day of operations, the emergency management director and several other county officials receive an email threatening to shut down the county's information networks unless a payment of $300,000 in bitcoin is made by the end of the day. Similar threats are received via the county's official social media sites. Shortly after the threats are received, the county government's email system and websites go offline for exactly 30 minutes, then come back online. Access to critical information databases is also lost, then restored. The hackers claim responsibility for the outage and threaten to increase the ransom amount and severity of attacks if the ransom payment is not received.

  **Inject Discussion**:

  Are IT disaster recovery and incident response plans in place? How are these plans activated?

  Are continuity of operations plans in place? How are these plans activated?

  How would an alternate EOC location be activated?

  Does the jurisdiction have cybersecurity insurance?

  Who has the authority to approve or deny the ransom payment? What is that process?

  What state or federal notifications or requests for assistance would be made?

  How is public information, social media, and news media messaging managed?

- **Scenario 9: Troubled Waters**

  **Target**: Water Utility Control Systems

  **Attack Method**: Industrial Control System Malware

  **Triggering Incident Description**:

  A local fire department responds to a large fire at the community's primary water treatment plant. Plant personnel report the fire started in an area of the plant that houses high lift water pumps. These pumps discharge treated drinking water into water mains and storage tanks for distribution. They also stated that just before the fire began, they were unable to access the computer system that controlled the pumps. The pumps began to cycle on and off, running at very high RPMs, then quickly shutting

down. Attempts to access the control systems on site and from remote computer terminals failed. After several minutes, all of the pumps in the plant burned out and failed, with one pump catching fire. The plant can no longer maintain pressure within the system, which provides water to most of the county and large portions of adjacent counties. Water sampling of storage tanks also showed dangerously high levels of chemicals used to disinfect water at the plant. During a detailed analysis of the control systems, highly sophisticated malware was detected. The malware had caused the pumps to malfunction, altered the amount of disinfectant used to treat the water, and locked operators out of the system. The water supply for residents, hospitals, schools, manufacturing, and firefighting is now unavailable, and will likely be offline for weeks.

**Inject Discussion**:

How would the county's response be activated and coordinated?

How would the community be notified of the incident and warned of water contamination?

How could InWARN mutual aid resources be requested?

Is local, state, and/or federal law enforcement notified?

What state and federal resources could be requested?

How could drinking water be distributed to the community?

How would water for healthcare facilities be provided?

Would evacuation of hospitals be necessary?

How would schools be affected?

How could water for firefighting be supplied?

How would wastewater treatment be impacted?

What are the potential sanitation and public health hazards?

Are there legal and regulatory issues that must be addressed?

How could weather conditions affect potential impacts and response operations? (i.e. Winter vs. Summer)

- **Scenario 10: The Blackout**

  **Target**: Electric Power Utilities

  **Attack Method**: Advanced Persistent Threat, Industrial Control System Malware

  **Triggering Incident Description**:

  It is late Monday afternoon, the day before Election Day. Weather is fair across the Midwest with no severe weather or extreme temperatures. At 4:45 PM EST, multiple

cable news networks begin to report a major power outage in the City of Detroit. Within 30 minutes of the initial news reports, widespread power outages are reported across Michigan, Wisconsin, Minnesota, and northern Ohio. At 5:40 PM power outages begin to occur across Central Illinois and Northwest Indiana.

At 6:15 PM, power outages occur across your entire county. Simultaneously, adjacent counties experience widespread outages. All fire stations, police stations, and healthcare facilities in the county are on generator power. The county public safety answering point and emergency operations center are also operating on generator power. 911 service is operational, but is quickly being overwhelmed by emergency calls and inquiries from the public. County Emergency Management is notified the Indiana State Emergency Operations Center is activated.

By 8:00 PM, multiple power companies and regional transmission organizations confirm massive power outages in seven states across the Midwest. The cause of the blackout, as well as when power will be restored, is unknown. Locally, nearly all traffic lights in the county are out. Numerous vehicle accidents and major traffic backups are reported. Grocery stores, gas stations, hardware, and home improvement stores are frantically requesting law enforcement assistance to deal with security and crowd control problems. Fire departments are responding to multiple fires at electric power substations and pole-mounted transformers across the county. EMS response is delayed due to the volume of calls and traffic congestion. Water and wastewater treatment plants remain operational, but are on emergency generator power. There are sporadic landline telephone and internet service outages, but cellular telephone systems are operating normally.

At 10:00 PM, the U.S. Department of Homeland Security (USDHS) confirms the power outages were caused by a massive cyberattack against power companies and regional power management organizations. The identity of the attacker and the method of attack are not announced.

In Indiana, it is estimated 90 % of the state is without electricity. Only a few counties in Northeastern Indiana have power. Areas of the Midwest not affected by the blackout include the City of Chicago and areas of Northern Illinois, Southwestern Michigan, and most of Central and Southern Ohio. The State of Kentucky is not impacted by the power outage. The Governor of Indiana formally declares a state of emergency, activates the National Guard, and requests federal assistance.

24 hours after the attack began, USDHS officials confirm the attack is sophisticated, coordinated, and consistent with the capabilities of a nation state. The President of the United States issues a Major Disaster Declaration. Cyber incident response operations have isolated and contained the impacts to the Midwest. Electrical power in the rest of the U.S. is unaffected. Across the Midwest, major physical damage to power generation plants, power transmission, and power distribution infrastructure has occurred. Due to the extent of the damage and compromise of control systems, the local electric power utility reports repair and power restoration in the county may not begin for two to three weeks. Full restoration of power to all areas of the county may take up to three months.

**Inject Discussion**:

How would the county's incident response be activated and coordinated?

How would Emergency Support Functions be mobilized and staffed?

How would situational awareness be established and maintained?

What are your jurisdiction's incident priorities, goals, and objectives?

What emergency response and continuity of operations plans are in place? How would these plans be implemented?

What are the immediate public safety, security, and health concerns?

How would critical county information networks and telecommunication systems be maintained and protected during an extended power outage. How would county and/or contract IT professionals be integrated into the incident response?

How would local elected officials be engaged? What emergency orders would need to be issued?

How would the county EOC establish and maintain communications with local, county, district, volunteer, state, and federal partners during a prolonged power outage?

How would resource needs be assessed and requests for assistance communicated?

How long can critical public safety, healthcare, water/wastewater utility, and telecommunications facilities operate on emergency generator power without refueling?

What are the anticipated fuel needs for vehicles and generators? What type of fuel is required?

How would public information, warnings, and alerts be managed and communicated?

How would critical staffing needs be met? (i.e. public safety, healthcare, mass care)

How would potable water be provided to the community if water utility systems fail?

How would natural gas utilities in your area be affected?

How would wastewater treatment and community waste management services be maintained?

How would transportation infrastructure and services be affected? (i.e. streets, highways, rail, airports, public transportation)

During a prolonged power outage lasting weeks or months, how would fuel distribution and fuel use be prioritized? How could community fuel rationing be implemented and maintained?

What could be done to help maintain retail food and fuel services at grocery stores and gas stations?

How would food be provided to the community if grocery stores could not remain open?

What are the anticipated long-term mass care and sheltering needs?

How would access and functional needs populations, residents of long-term care facilities, and those in home healthcare programs receive assistance?

What is the impact on local school systems?

How would volunteers and donations be managed?

What are the potential financial issues that would need to be addressed? (i.e. county employee payroll, purchasing, cost tracking, damage costs, documentation, bank closures)

What government and social services could be maintained? (i.e. courts, county offices, WIC)

How would the election, scheduled for the day after the attack occurred, be affected?

How would local government assist power companies in repairing damaged infrastructure?

Once damaged equipment was repaired and control systems brought back online, how would local government agencies support the safe reenergizing of the local power grid and restoration of power?

How would economic impacts to the community be mitigated? How would long-term recovery activities be managed?

How would county and/or contract IT professionals be integrated into long-term recovery activity?

## F. Evaluation and Improvement

The evaluation phase for all exercises includes a formal exercise evaluation, an integrated analysis, and an After Action Report/Improvement Plan (AAR/IP) that identifies strengths and areas for improvement of an agency's preparedness, based on exercise performance. Recommendations developed during evaluation are used in improvement planning phase.

During improvement planning, the corrective actions identified in the evaluation phase are assigned, with due dates, to responsible parties; tracked to implementation; and then validated during subsequent exercises.

The importance of applying lessons learned, from both successes and failures, cannot be overstated. True cybersecurity preparedness can only be accomplished through a constant cycle of effective planning, training, exercise, and improvement

## IV. Information Resources for Training and Exercise

Indiana Cybersecurity Hub
www.in.gov/cyber

Indiana Cybersecurity Hub – Emergency Response and Recovery
https://www.in.gov/cybersecurity/3813.htm

Indiana Information Sharing and Analysis Center (IN-ISAC)
https://www.in.gov/cybersecurity/in-isac/

Indiana Department of Homeland Security Exercise Guide
https://www.in.gov/dhs/files/IDHS-Exercise-Guide-v4.pdf

FEMA National Training and Education Division (NTED)
https://www.firstrespondertraining.gov/frts/npccatalog

Homeland Security Exercise and Evaluation Program (HSEEP) Toolkit
https://preptoolkit.fema.gov/hseep-resources

Industrial Control Systems Cyber Emergency Response Team (ICS CERT) Training
https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

United States Cyber Emergency Response Team (US CERT) Training
https://niccs.us-cert.gov/training

National Institute of Standards and Technology (NIST) Cybersecurity Framework
https://www.nist.gov/cyberframework

## V. Guide Development and Maintenance

This Guide was developed by the Emergency Services and Exercise Subcommittee of the State of Indiana Governor's Executive Council on Cybersecurity. The Subcommittee was chaired by the Executive Director of the Indiana Department of Homeland Security. Subcommittee members included multi-disciplinary representatives from public sector, private sector, and academic organizations including:

- Citizens Energy Group
- Indiana American Water
- Indiana Department of Homeland Security
- Indiana Department of Transportation
- Indiana Statewide 911 Board
- Indiana University
- Indiana University Health
- Ivy Tech Community College
- Resilient Strategies, LLC
- Ritter Strategic Services

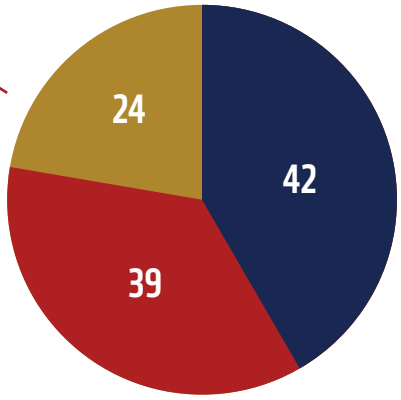
The Guide will be reviewed, revised, and maintained by the Indiana Department of Homeland Security, in collaboration with the members of the Emergency Services and Exercise Subcommittee, and at the direction of the Cybersecurity Program Director.


# CYBERSECURITY ATTACKS IN INDIANA: QUICK RESPONSE GUIDE

# CYBERSECURITY ATTACKS IN INDIANA: QUICK RESPONSE GUIDE

**105** total breaches reported over the last 12 months

**94%** of malware continues via email




**42** State, County and Municipalities Government

**39** K-12 and Higher Education

**24** County / Local Healthcare (not privately owned)

## REPORT A CYBER CRIME

When an organization's experiencing a cyber attack, follow these steps to report the cyber crime.

### STEP 1 - CONTACT LAW ENFORCEMENT

- FBI Internet Crime Complaint Center (IC3) Alert authorities of suspected criminal or civil violations.
- **Indiana State Police (ISP)** Cybercrime & Investigative Technologies specialize in conducting cyber crime investigations.
- If there is an immediate threat to public health or safety, call 911.

### STEP 2 - ADDITIONAL REPORTING SUCH AS:

- **Indiana Attorney General** requires organizations report any security breach resulted in exposure of personal information. For more information, click here.
- **Regulators:** Regulated organizations may need to report cyber crimes to other state or federal agencies.
- **Secretary of State:** If necessary, contact the SOS offices regarding any related cyber incidents at electionsecurity@sos.in.gov.
- **Federal Government:** This fact sheet explains how to report cyber crimes to many federal agencies.

### STEP 3 - UTILIZE ADDTIONAL RESOURCES

Utilize additional resources about tips regarding avoiding ransomware, National Governors Association Response Planning Memo, National Emergency Readiness Team information, Department of Homeland Security's National Cybersecurity and Communications Integration Center, and more for 24/7 cyber situational awareness, incident response, and management center at www.in.gov/cybersecurity/3807.htm.

### STEP 4 - INFORMATION SHARING

It's important to share cyber crime information with other organizations to protect critical infrastructure, the State of Indiana, and our nation. Learn more at www.in.gov/cybersecurity/3819.htm.

***Source: HIPPA Breach reporting, public news, Indiana Attorney General Breach reporting from July 2018 – July 2019; 2019 Verizon Data Breach Report**

# CYBERSECURITY ATTACKS IN INDIANA: QUICK RESPONSE GUIDE

## THREE STEPS TO RESILIENCY AGAINST RANSOMWARE NOW

### STEP 1 - BACK UP YOUR SYSTEM - NOW AND DAILY

Immediately and regularly back up all critical agency and system configuration information on a separate device and store the back-ups offline, verifying their integrity and restoration process. If recovering after an attack, restore a stronger system than you lost, fully patched and updated to the latest version.

### STEP 2 - REINFORCE BASIC CYBERSECURITY AWARENESS AND EDUCATION

Ransomware attacks often require the human element to succeed. Refresh employee training on recognizing cyber threats, phishing and suspicious links – the most common vectors for ransomware attacks. Remind employees of how to report incidents to appropriate information technology staff in a timely manner, which should include out-of-band communication paths.

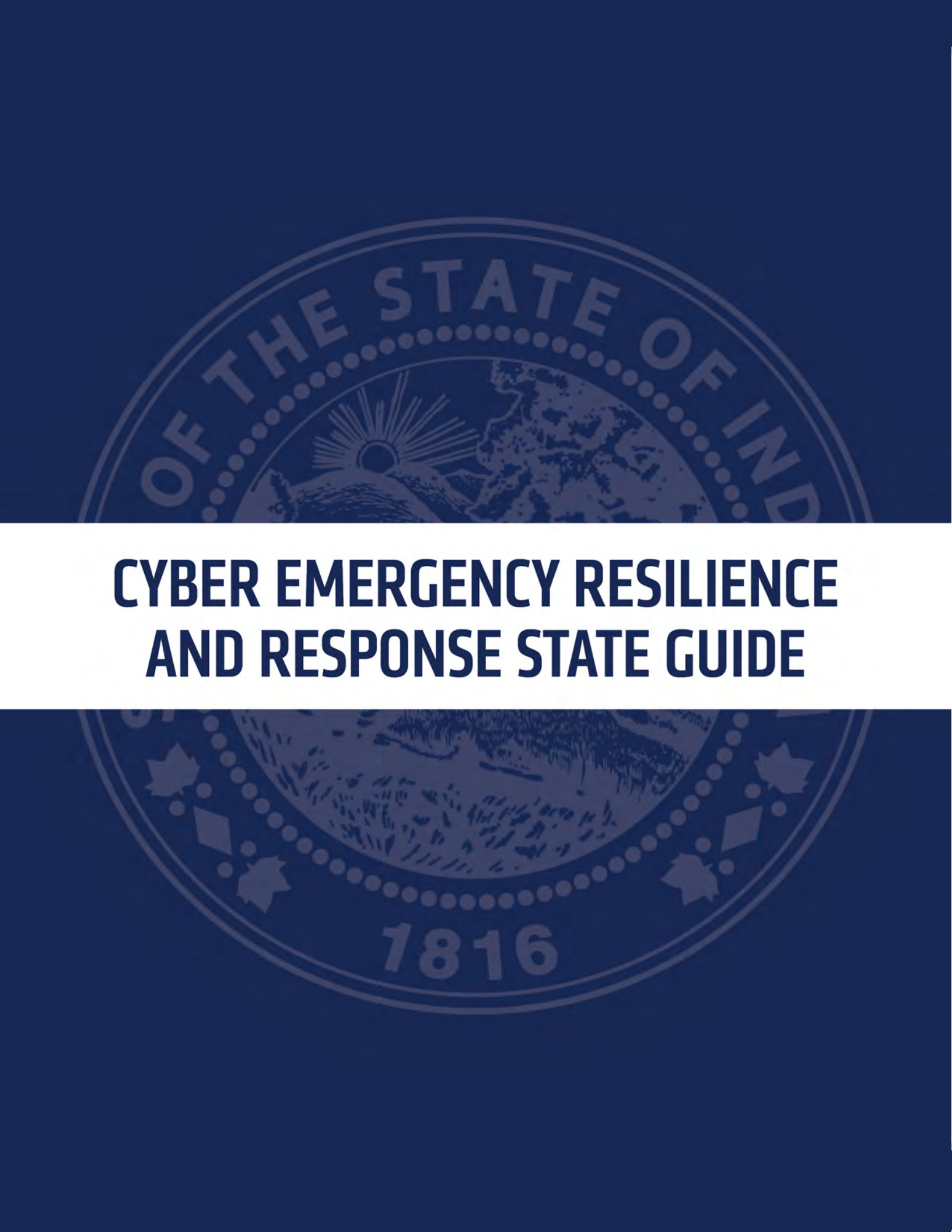
### STEP 3- REVISIT AND REFINE CYBER INCIDENT RESPONSE PLANS

Agencies must have a clear plan to address attacks when they occur, including when internal capabilities are overwhelmed. Make sure response plans include how to request assistance from external cyber first responders, such as state agencies, CISA and the MS-ISAC, in the event of an attack.

## EMERGENCY MANAGER RESOURCES

To find cybersecurity toolkit, planning templates, guides, resources, and more for emergency managers, visit https://www.in.gov/cybersecurity/3818.htm.

***Source: HIPPA Breach reporting, public news, Indiana Attorney General Breach reporting from July 2018 – July 2019; 2019 Verizon Data Breach Report**




# CYBER EMERGENCY RESILIENCE AND RESPONSE STATE GUIDE

# CYBER EMERGENCY RESILIENCY AND RESPONSE STATE GUIDE

## Table of Contents

## 1.0 Introduction and Definitions

The Indiana Cyber Emergency Resiliency and Response State Guide (State Guide) was created to communicate the roles of an effective emergency response to a cyber emergency from the Executive Branch of Indiana government and indicate what roles partners may have during a cyberattack.

Determining which organizations should be involved and the roles they will play has proven challenging at all levels of government for nontraditional catastrophic emergencies such as a cyber attack. Emergency managers often have a difficult time understanding the technical nature of a cyber attack and how that fits in an emergency response while still developing decision-making processes that are true to an all-hazards approach. Below are emergency management resources to assist in planning and responding to a cyber attack.

### Cyber Emergency VS Cyber Incident

The State of Indiana defines a **cyber emergency** as any actual, imminent, or potential incident that will adversely affect public health, safety, or security; the environment; or economic prosperity on a level materially significant to the State of Indiana or its operations that requires a coordinated state response.

The State of Indiana defines a **cyber incident** as it is described in the Presidential Policy Directive 41, which is "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical, or virtual infrastructure controlled by computers or information systems, or information resident thereon."

## 2.0 Purpose

The State Guide the roles, considerations, and process to effectively coordinate the proper resources to proactively protect and defend state-owned data systems and networks during a cyber emergency. This will also provide clarification to the state's role in assisting local units of government in a cyber-related incident as well as coordinating with private sector partners.

## 3.0 Scope

The State Guide will be utilized when the following criteria are met:

- A cyber emergency involving activation of state level continuity of operations (COOP), or continuity of government (COG) plans.
- A cyber event that has a material impact on public safety.
- A threat or incident involving state-level, cyber-critical infrastructure.
- When requested by:
    - A local government entity
    - Director of the Indiana Office of Technology
    - Director of the Department of Homeland Security
    - The Adjutant General of Indiana

- When directed by:
    - The Governor of Indiana

## 4.0 Cyber Emergency Resiliency and Response Partners

The State of Indiana relies on a core group of agencies to assess the circumstances, determine an emergency, and deliver the response needed from state government. Inclusion in the core group is driven by the essential expertise and capabilities needed from the Executive Branch to assess and potentially assist in a response to the cyber emergency situation. As with many other threats and hazards, the success of resiliency and response must rely on the state, federal, public, military, and private partners.

### STATE AGENCIES AND PARTNERS

#### OFFICE OF THE GOVERNOR

The Governor provides overall direction and control for the preparation and carrying out of all emergency actions, including development and execution of the State's Comprehensive Emergency Management Plan. State agencies will support emergency operations in accordance with Executive Order 17-02.

#### INDIANA DEPARTMENT OF HOMELAND SECURITY

IDHS is tasked to coordinate the state's emergency plans, and serve as the coordinating agency for state efforts for preparedness for, response to, mitigation of, and recovery from emergencies and disasters. As with other hazard-related emergencies, IDHS manages the operations of the State Emergency Operations Center.

#### INDIANA OFFICE OF TECHNOLOGY

IOT oversees and manages the IN-ISAC. IOT is responsible for the security of state government information networks and all domains and is responsible for protecting the State's IT infrastructure from internal and external cybersecurity threats. IOT will assist IDHS during an cyber emergency activation with situational awareness, identifying external decision-makers, and accessing the necessary mitigation resources and lead remediation efforts if the event affected state government infrastructure.

#### INDIANA STATE POLICE

The ISP Office of Intelligence and Investigative Technologies (OIIT) focuses on cybersecurity incidents with a criminal nexus. The Cybersecurity Crime and Investigative Technologies Section and the Crime Analysis Section conduct activities related to cybersecurity forensics, cybersecurity crime investigations including those involving network intrusion and exploitation, electronic surveillance, and crimes against children.

The Indiana Intelligence Fusion Center (IIFC) collaborates with the IN-ISAC to conduct criminal intelligence analysis and incident reporting involving cybersecurity crimes. In the event that a criminal nexus is suspected in a cybersecurity emergency, law enforcement will investigate. Post-recovery, the IIFC may work with the IN-ISAC to help generate analytical after-action reports for external partners.

### INDIANA NATIONAL GUARD

The INNG has a Cybersecurity Mission comprised of experts in both preparedness and response efforts. As with other state emergencies, IDHS Executive Director may request deployment of cybersecurity force packages to support incident response.

### INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Signed by Governor Eric. J Holcomb on January 9, 2017, the Indiana Executive Council on Cybersecurity (IECC or 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 more than 250 advisory members, the Council delivered a comprehensive strategy plan to Governor Holcomb September 2018.

Moreover, the experts of the Council are charged with providing best practices, resources, and information to increase the state resiliency against cyberattacks. In addition to the private and public partners, state agencies and elected officials such as the Indiana Economic Development Corporation, Indiana Secretary of State, Indiana Attorney General, and many more have come together to increase the resiliency.

In a cyber emergency, experts from the Council may be included as a part of the Cybersecurity Advisory Group.

### CYBERSECURITY ADVISORY GROUP

The Indiana Cybersecurity Advisory Group (CAG) provides operational guidance and subject-matter expertise in support of a coordinated state cybersecurity incident response. The CAG will assess the incident and organize the strategic response to give to IDHS's Emergency Operations Center. The CAG also develops, coordinates and recommends courses of action and response strategies. Designated agency representatives include the IOT Chief Information

Security Officer, or designee, ISP Commander, Intelligence and Investigative Technologies or designee, INNG Defensive Cybersecurity Programs Lead, or designee, Indiana Cybersecurity Program Director, IDHS Division Director, Response and Recovery, or designee and selected subject-matter experts.

## FEDERAL AGENCIES

### U.S. DEPARTMENT OF HOMELAND SECURITY

The Department of Homeland Security (DHS) is the designated lead agency during a cybersecurity incident requiring a federal response. Their primary functions are to identify the source of disruption and help remove it, determine how they gained access, assess the damage, and provide guidance to the organization on how to make their system more secure.

### FEDERAL BUREAU OF INVESTIGATIONS

The FBI is the lead federal agency for investigating cybersecurity-attacks by criminals, overseas adversaries, and terrorists. Specially trained FBI agents and analysts based at the FBI Indianapolis Field Office investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud.

### U.S. SECRET SERVICE

The Secret Service maintains Electronic Crimes Task Forces, which focus on identifying and locating international cybersecurity criminals connected to cybersecurity intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cybersecurity training and information to combat cybersecurity crime.

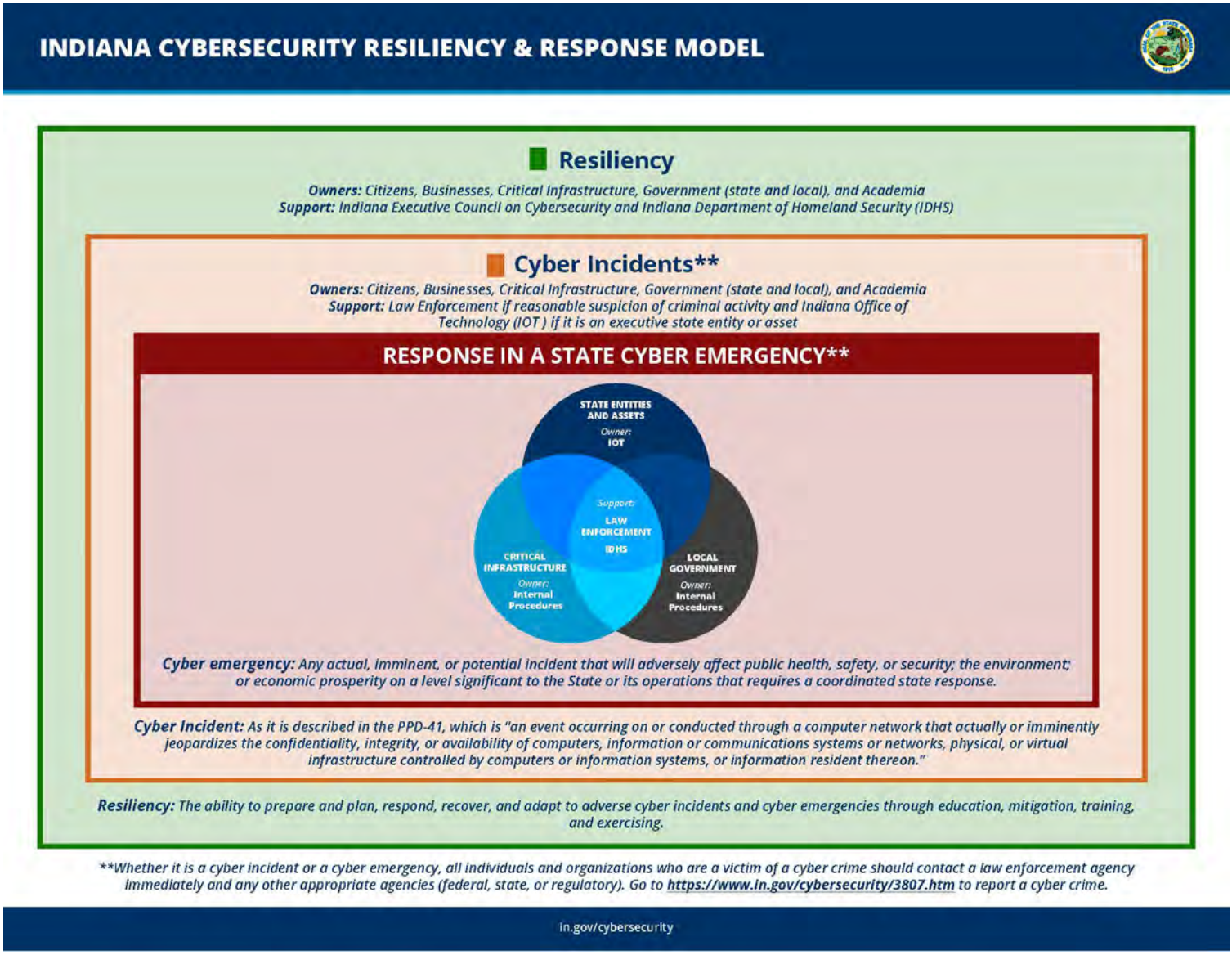
### U.S. DEPARTMENT OF JUSTICE

DOJ’s Offices of U.S. Attorneys and its’ Criminal and National Security Divisions, working with federal law enforcement agencies, use criminal and national security authorities to investigate, prosecute, and disrupt cyber threats and to apprehend cyber threat actors. Information and evidence obtained pursuant to appropriate legal process are used to identify the source of cyber incidents and to gather pertinent cyber threat information.

## 5.0 Cyber Emergency Resiliency Efforts

The State of Indiana core agency group include the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana National Guard, and Indiana State Police.

This core agency group assists and leads in the overseeing of the cybersecurity resiliency efforts of the Indiana Executive Council on Cybersecurity and the ability for the state to be prepared to enable the rapid and effective response needed by state government constituents during a cyber emergency or cyber incident as appropriate. The following Indiana Cybersecurity Resiliency and Response Model further identifies the owners and support organizations during the resiliency phase, a cyber incident, and a cyber emergency.



## 6.0 Response Process

### Report a Cyber Crime

When an organization's experiencing a cyber attack, the following these steps should be taken.

Step 1: Contact Law Enforcement

- FBI Internet Crime Complaint Center (IC3)
- Indiana State Police (ISP) Cybercrime and Investigative Technologies
- If there is an immediate threat to public health or safety, call 911.

Step 2: Additional Reporting

In addition to reporting the cyber attack, an organization should consider contacting other agencies to report the attack, which include:

- **Indiana Attorney General** requires organizations report any security breach resulted in exposure of personal information. For more information, click here.
- **Regulators:** Regulated organizations may need to report cyber crimes to other state or federal agencies.
- **Secretary of State:** If necessary, contact the SOS offices regarding any related cyber incidents at electionsecurity@sos.in.gov
- **Federal Government:** This fact sheet explains how to report cyber crimes to many federal agencies.
- **Indiana Department of Homeland Security** at WatchDesk@dhs.IN.gov.

Step 3: Utilize additional resources

For additional tips regarding avoiding ransomware and information from the National Governors Association Response Planning Memo, National Emergency Readiness Team information, Department of Homeland Security's National Cybersecurity and Communications Integration Center, and more visit www.in.gov/cybersecurity/3807.htm.

Step 4: Information Sharing

It's important to share cyber crime information with other organizations to protect critical infrastructure, the State of Indiana, and our nation. Learn more at www.in.gov/cybersecurity/3819.htm.

It is important to note that once the State of Indiana is notified, the following process was created with a single objective: Get the emergency into the hands of capable, representative, and empowered individuals to bring Indiana government resources and relationships quickly to the aid of those suffering from a cyber emergency.

Once a request for assistance is received by one or more state agencies, the core agency group will convene and assess the traits and impacts of the cyber incident or emergency and the value of their resources as they apply to an effective response to the emergency, whether it is with state resources or working with other key public and private partners. Cyberattacks shared with the State of Indiana will stay at the highest level of leadership and only shared with need-to-know parties. After each cyber event reported to one or more of the core agency group, a post-emergency evaluation will be completed by the state's Cybersecurity Program Director to rate response effectiveness, identify additional needs, and process adjustments.

## 7.0 Plan Maintenance

The State of Indiana Department of Homeland Security Executive Director, Indiana Office of Technology Chief Information Officer (CIO), and Indiana Cybersecurity Program Director are responsible for overall administration and maintenance of this State Guide.

# ADDITIONAL EMERGENCY MANAGER CYBERSECURITY RESOURCES

# ADDITIONAL EMERGENCY MANAGER CYBERSECURITY RESOURCES

Below you will find a variety of additional resources for emergency managers regarding preparing, responding, and recovering from a cyberattack.

- MS-ISAC Security Primer on Ransomware
- US DHS Cybersecurity and Infrastructure Security Agency (CISA) Ransomware Website
- National Governors Association Disruption Response Planning Memo
- NASCIO Cyber Disruption Planning Guide
- Emergency Services Sector Cybersecurity Initiative
  A Department of Homeland Security resource to better understand and manage cyber risks and to coordinate the sharing of cyber information and tools between subject matter experts (both inside and outside the federal government) and the Emergency Services Sector disciplines.
- Emergency Services Sector Cybersecurity Framework Implementation Guidance
- US DHS Emergency Services Sector Cybersecurity Best Practices
- Ready.gov
  Ready.gov is a national public service campaign designed to educate and empower the American people to prepare for, respond to, and mitigate emergencies, including cybersecurity.
- US DHS Cybersecurity and Infrastructure Security Agency (CISA) Cyber Resilience Review (CRR)
  The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.
  - Information Sheet - Summary of the CRR process.
  - Method Description and User Guide - Walk-through for how an organization can conduct a CRR self-assessment.
  - Self-Assessment Package - Self-assessment form and report generator.
  - Question Set with Guidance - Self-assessment question set along with accompanying guidance.
  - CRR NIST Framework Crosswalk - Cross-reference chart for how the NIST Cybersecurity Framework aligns to the CRR.
- National Cyber Incident Response Plan (NCIRP)
  The NCIRP, developed by the United States Computer Emergency Readiness Team (US-CERT), describes a national approach to dealing with cyber incidents; addresses the important role that the private sector, state and local governments, and multiple federal agencies play in responding to incidents and how the actions of all fit together for an integrated response.
- National Cybersecurity and Communications Integration Center (NCCIC)
  A 24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement.

For more information for individuals, businesses, government, educators, and more, visit www.in.gov/cyber.

# BIBLIOGRAPHY

# BIBLIOGRAPHY

In addition to the following resources used to create the *Indiana Emergency Manager Cybersecurity Toolkit*, a significant amount of work and resources were from the experts from the Indiana Executive Council on Cybersecurity, feedback from Indiana Emergency Managers at all levels (city, county, district, private, and state), and national partner agencies such as US Department of Homeland Security, FEMA, National Governors Association Cybersecurity Academy, CIA, FBI, US Secret Service, and National Guard.

Research conducted to develop this toolkit also included information from the following organizations:

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.

Cybersecurity and Infrastructure Security Agency (CISA): Responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

Executive Order 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Emphasizes four core areas: securing and modernizing federal networks, protecting the critical infrastructure that maintains the American way of life, deterring America's adversaries in cyberspace, and building a stronger cybersecurity workforce.

*Other more specific citied references include, but are not limited to:*


Federal Emergency Management Agency (FEMA). "National Incident Management System (NIMS)," October 2017. https://www.fema.gov/national-incident-management-system. (accessed September 2018)

Emergency Management Accreditation Program (EMAP). "Emergency Management Accreditation Program (EMAP)," 2001. https://www.emap.org/ (accessed September 2018).

National Fire Protection Association (NFPA) Standard 1600. "NFPA Standard 1600," June 2018. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600 (accessed September 2018).

Centers for Medicare and Medicaid Services (CMS). "Emergency Preparedness Rule," November 16, 2016. https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule.html (accessed September 2018)

The Joint Commission. "Emergency Management Standard," https://www.jointcommission.org/emergency_management.aspx (accessed September 2018)

The White House. "Presidential Policy Directive -- United States Cyber Incident Coordination (PPD 41)" July 26, 2016.: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential- policy-directive-united-states-cyber-incident (accessed September 2018)

Federal Emergency Management Agency (FEMA). "Homeland Security Exercise Evaluation Program (HSEEP)", https://www.fema.gov/hseep (accessed September 2018)

U.S. Department of Health and Human Services. “Health Insurance Portability and Accountability Act (HIPAA) Security Rule”, February 20, 2003. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (accessed September 2018)

U.S. Department of Homeland Security (DHS). “U.S. Computer Emergency Readiness Team (US-CERT)”., https://www.us- cert.gov/ (accessed September 2018)

Communications Sector Coordinating Council (CSCC) and Communications Sector Government Coordinating Council (CGCC). “Communications Sector-Specific Plan.” *Cybersecurity and Infrastructure Security Agency*. Department of Homeland Security and, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf. (accessed October 2019)

Dams Sector Coordinating Council (CSCC) and Dams Sector Government Coordinating Council (DGCC). “Dams Sector-Specific Plan.” *Cybersecurity and Infrastructure Security Agency*. Department of Homeland Security, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf. (accessed October 2019)

Emergency Services Sector Coordinating Council (ESSCC) and Emergency Services Sector Government Coordinating Council (ESSGCC). “Emergency Services Sector-Specific Plan.” *Cybersecurity and Infrastructure Security Agency*. Department of Homeland Security and, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-emergency-services-2015-508.pdf. (accessed October 2019)

U.S. Department of Energy (DOE). “Energy Sector-Specific Plan - 2015 | CISA.” Cisa.gov, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf. (accessed October 2019)

Department of Homeland Security (DHS) and the General Services Administration (GSA). “Government Facilities SSP - 2015 | CISA.” Cisa.gov, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf. (accessed October 2019)

Healthcare and Public Health (HPH) Sector Coordinating Council (SCC) and Government Coordinating Council (GCC). “Healthcare Sector-Specific Plan - 2015 | CISA.” Cisa.gov, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf. (accessed October 2019)

Water Sector Coordinating Council and the Water Sector Government Coordinating Council. “Water Sector-Specific Plan - 2015 | CISA.” Cisa.gov, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf. (accessed October 2019)

U.S. Department of Homeland Security (DHS)—with the Transportation Security Administration and the United States Coast Guard as executive agents for DHS—and the U.S. Department of Transportation. “Transportation Systems Sector | CISA.” Cisa.gov, 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf. (accessed October 2019)

Election Infrastructure Subsector. “Election Security.” Department of Homeland Security, March 27, 2018. https://www.dhs.gov/topic/election-security. (accessed October 2019)

Wikipedia contributors, "Voice over IP," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Voice_over_IP&oldid=921717372 (accessed October 2019).

Wikipedia contributors, "Plain old telephone service," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Plain_old_telephone_service&oldid=920489716 (accessed October 2019).

Wikipedia contributors, "Satellite phone," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Satellite_phone&oldid=918760438 (accessed October 2019).

Wikipedia contributors, "Professional mobile radio," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Professional_mobile_radio&oldid=899043563 (accessed October 2019).

Wikipedia contributors, "Radio over IP," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Radio_over_IP&oldid=918341989 (accessed October 2019).

DotGov Program. “Domain Requirements | DotGov.” Dotgov.gov, 2018. https://home.dotgov.gov/registration/requirements/. (accessed October 2019)

Parker, Melly. "Differences Between Personal and Corporate-Based Email" accessed October 2019. http://smallbusiness.chron.com/differences-between-personal-corporatebased-email-60187.html

Wikipedia contributors, "Local area network," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Local_area_network&oldid=919579589 (accessed October 2019).

Wikipedia contributors, "Wireless LAN," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Wireless_LAN&oldid=919969383 (accessed October 2019).

Wikipedia contributors, "Internet service provider," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Internet_service_provider&oldid=920723956 (accessed October 2019).

Margaret Rouse and Ivy Wigmore, “mobile hotspot”, *WHatIs.com,* https://whatis.techtarget.com/definition/mobile-hotspot (accessed October 2019)

Wikipedia contributors, "Intranet," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Intranet&oldid=919727563 (accessed October 2019).

Wikipedia contributors, "Website," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Website&oldid=921401825 (accessed October 2019).

Wikipedia contributors, "Extranet," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Extranet&oldid=911699334 (accessed October 2019).

Department of Homeland Security. “Safeguarding Sensitive but Unclassified (For Official Use Only).” Management Directive System. Department of Homeland Security, November 5, 2004. https://fas.org/sgp/othergov/dhs-sbu.html. (accessed October 2019)

U.S. Government Accountability Office, “Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information,” *Gao.Gov*, no. GAO-06-385 (2009), https://www.gao.gov/products/GAO-06-385. (accessed October 2019)

GovRegs, “6 CFR 29.8 - Disclosure of Protected Critical Infrastructure Information.,” Govregs.com, 2019, https://www.govregs.com/regulations/expand/title6_chapterI_part29_section29.8. (accessed October 2019)

Wikipedia Contributors, “Vital Record,” Wikipedia (Wikimedia Foundation, July 13, 2019), https://en.wikipedia.org/wiki/Vital_record. (accessed October 2019)

HIPAA Journal, “What Is Protected Health Information?,” HIPAA Journal, January 10, 2018, https://www.hipaajournal.com/what-is-protected-health-information/. (accessed October 2019)

Black's Law Dictionary, "What Is COURT RECORD? Definition of COURT RECORD (Black's Law Dictionary)," The Law Dictionary (The Law Dictionary, March 28, 2013), https://thelawdictionary.org/court-record/. (accessed October 2019)

Connor Reporting, "Court Records and Proceedings: What Is Public and Why? - Connor Reporting," Connor Reporting, April 18, 2017, https://connorreporting.com/court-records-proceedings-public/. (accessed October 2019)

*A Law Dictionary, Adapted to the Constitution and Laws of the United States. By John Bouvier.*. S.v. "contract." Retrieved October 2019 from https://legal-dictionary.thefreedictionary.com/contract. (accessed October 2019)

"Different Types of Contracts: Everything You Need to Know," UpCounsel, 2019, https://www.upcounsel.com/different-types-of-contracts. (accessed October 2019)

Payment Card Industry Security Standards Council, "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards," Pcisecuritystandards.org, May 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf. (accessed October 2019)

Federal Trade Commission (FTC). "Identity Theft Recovery Steps | IdentityTheft.Gov." Identitytheft.gov. IdentityTheft.gov, 2019. https://www.identitytheft.gov/Info-Lost-or-Stolen. (accessed October 2019)

Orszag, Peter. "Executive Office of The President Office of Management And Budget M-10-23 Memorandum For The Heads Of Executive Departments And Agencies From." *Privacy Laws, Policies and Guidance*. Office of Management and Budget, June 25, 2010. http://www.osec.doc.gov/opog/privacy/Memorandums/OMB_M-10-23.pdf. (accessed October 2019)

Wikipedia contributors, "Data center," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Data_center&oldid=920876767 (accessed October 2019).

Wen, Howard. "Cloud vs. Data Center: What to Consider." Business News Daily, December 27, 2018. https://www.businessnewsdaily.com/4982-cloud-vs-data-center.html. (accessed October 2019)

Techopedia. "What Is a Managed Data Center? - Definition from Techopedia." Techopedia.com, October 2019. https://www.techopedia.com/definition/30134/managed-data-center. (accessed October 2019)

Techopedia. “What Is Network Infrastructure? - Definition from Techopedia.” Techopedia.com, October 2019. https://www.techopedia.com/definition/16955/network-infrastructure. (accessed October 2019)

Wikipedia contributors, "Server (computing)," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Server_(computing)&oldid=918793041 (accessed October 2019).

Wikipedia contributors, "Desktop computer," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Desktop_computer&oldid=920206934 (accessed October 2019).

Wikipedia contributors, "Laptop," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Laptop&oldid=921740639 (accessed October 2019).

Wikipedia contributors, "Tablet computer," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Tablet_computer&oldid=920705015 (accessed October 2019).

Wikipedia contributors, "File server," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=File_server&oldid=920749909 (accessed October 2019).

WhatIs.com. “What Is Hard-Drive Encryption? Definition from WhatIs.Com.” Search Enterprise Desktop, 2019. https://searchenterprisedesktop.techtarget.com/definition/hard-drive-encryption. (accessed October 2019)

Wikipedia contributors, "Printer (computing)," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Printer_(computing)&oldid=921263048 (accessed October 2019).

Techopedia, “What Is a Scanner? - Definition from Techopedia,” Techopedia.com, October 2019, https://www.techopedia.com/definition/30441/scanner. (accessed October 2019)

Wikipedia contributors, "Image scanner," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Image_scanner&oldid=921115371 (accessed October 2019).

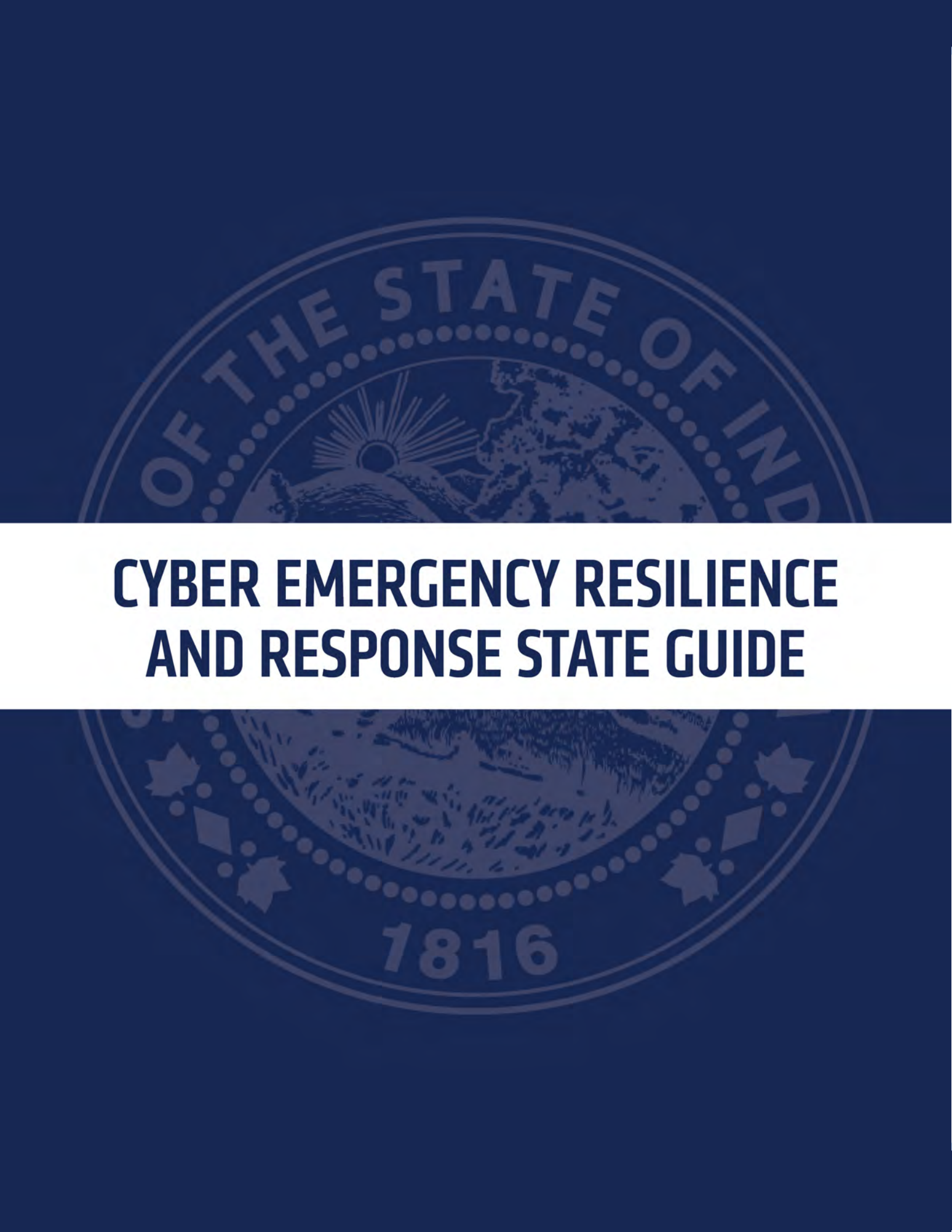
Wilson, Sarah, Sonia Lelii, and Margaret Rouse. “What Is USB Flash Drive? - Definition from WhatIs.Com.” SearchStorage, October 2019. https://searchstorage.techtarget.com/definition/USB-drive. (accessed October 2019)

WhatIs.com. “What Is External Hard Drive? - Definition from WhatIs.Com.” WhatIs.com. WhatIs.com, October 2019. https://whatis.techtarget.com/definition/external-hard-drive. (accessed October 2019)

Wikipedia contributors, "CD-ROM," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=CD-ROM&oldid=921638376 (accessed October 2019).

Wikipedia contributors, "Mobile phone," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Mobile_phone&oldid=921882355 (accessed October 2019).

# Indiana Cyber Emergency Resiliency Response State Guide




# CYBER EMERGENCY RESILIENCE AND RESPONSE STATE GUIDE

# CYBER EMERGENCY RESILIENCY AND RESPONSE STATE GUIDE

## Table of Contents

## 1.0 Introduction and Definitions

The Indiana Cyber Emergency Resiliency and Response State Guide (State Guide) was created to communicate the roles of an effective emergency response to a cyber emergency from the Executive Branch of Indiana government and indicate what roles partners may have during a cyberattack.

Determining which organizations should be involved and the roles they will play has proven challenging at all levels of government for nontraditional catastrophic emergencies such as a cyber attack. Emergency managers often have a difficult time understanding the technical nature of a cyber attack and how that fits in an emergency response while still developing decision-making processes that are true to an all-hazards approach. Below are emergency management resources to assist in planning and responding to a cyber attack.

### Cyber Emergency VS Cyber Incident

The State of Indiana defines a **cyber emergency** as any actual, imminent, or potential incident that will adversely affect public health, safety, or security; the environment; or economic prosperity on a level materially significant to the State of Indiana or its operations that requires a coordinated state response.

The State of Indiana defines a **cyber incident** as it is described in the Presidential Policy Directive 41, which is "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical, or virtual infrastructure controlled by computers or information systems, or information resident thereon."

## 2.0 Purpose

The State Guide the roles, considerations, and process to effectively coordinate the proper resources to proactively protect and defend state-owned data systems and networks during a cyber emergency. This will also provide clarification to the state's role in assisting local units of government in a cyber-related incident as well as coordinating with private sector partners.

## 3.0 Scope

The State Guide will be utilized when the following criteria are met:

- A cyber emergency involving activation of state level continuity of operations (COOP), or continuity of government (COG) plans.
- A cyber event that has a material impact on public safety.
- A threat or incident involving state-level, cyber-critical infrastructure.
- When requested by:
    - A local government entity
    - Director of the Indiana Office of Technology
    - Director of the Department of Homeland Security
    - The Adjutant General of Indiana

- When directed by:
    - The Governor of Indiana

## 4.0 Cyber Emergency Resiliency and Response Partners

The State of Indiana relies on a core group of agencies to assess the circumstances, determine an emergency, and deliver the response needed from state government. Inclusion in the core group is driven by the essential expertise and capabilities needed from the Executive Branch to assess and potentially assist in a response to the cyber emergency situation. As with many other threats and hazards, the success of resiliency and response must rely on the state, federal, public, military, and private partners.

### STATE AGENCIES AND PARTNERS

#### OFFICE OF THE GOVERNOR

The Governor provides overall direction and control for the preparation and carrying out of all emergency actions, including development and execution of the State's Comprehensive Emergency Management Plan. State agencies will support emergency operations in accordance with Executive Order 17-02.

#### INDIANA DEPARTMENT OF HOMELAND SECURITY

IDHS is tasked to coordinate the state's emergency plans, and serve as the coordinating agency for state efforts for preparedness for, response to, mitigation of, and recovery from emergencies and disasters. As with other hazard-related emergencies, IDHS manages the operations of the State Emergency Operations Center.

#### INDIANA OFFICE OF TECHNOLOGY

IOT oversees and manages the IN-ISAC. IOT is responsible for the security of state government information networks and all domains and is responsible for protecting the State's IT infrastructure from internal and external cybersecurity threats. IOT will assist IDHS during an cyber emergency activation with situational awareness, identifying external decision-makers, and accessing the necessary mitigation resources and lead remediation efforts if the event affected state government infrastructure.

#### INDIANA STATE POLICE

The ISP Office of Intelligence and Investigative Technologies (OIIT) focuses on cybersecurity incidents with a criminal nexus. The Cybersecurity Crime and Investigative Technologies Section and the Crime Analysis Section conduct activities related to cybersecurity forensics, cybersecurity crime investigations including those involving network intrusion and exploitation, electronic surveillance, and crimes against children.

The Indiana Intelligence Fusion Center (IIFC) collaborates with the IN-ISAC to conduct criminal intelligence analysis and incident reporting involving cybersecurity crimes. In the event that a criminal nexus is suspected in a cybersecurity emergency, law enforcement will investigate. Post-recovery, the IIFC may work with the IN-ISAC to help generate analytical after-action reports for external partners.

## INDIANA NATIONAL GUARD

The INNG has a Cybersecurity Mission comprised of experts in both preparedness and response efforts. As with other state emergencies, IDHS Executive Director may request deployment of cybersecurity force packages to support incident response.

## INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Signed by Governor Eric. J Holcomb on January 9, 2017, the Indiana Executive Council on Cybersecurity (IECC or 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 more than 250 advisory members, the Council delivered a comprehensive strategy plan to Governor Holcomb September 2018.

Moreover, the experts of the Council are charged with providing best practices, resources, and information to increase the state resiliency against cyberattacks. In addition to the private and public partners, state agencies and elected officials such as the Indiana Economic Development Corporation, Indiana Secretary of State, Indiana Attorney General, and many more have come together to increase the resiliency.

In a cyber emergency, experts from the Council may be included as a part of the Cybersecurity Advisory Group.

## CYBERSECURITY ADVISORY GROUP

The Indiana Cybersecurity Advisory Group (CAG) provides operational guidance and subject-matter expertise in support of a coordinated state cybersecurity incident response. The CAG will assess the incident and organize the strategic response to give to IDHS's Emergency Operations Center. The CAG also develops, coordinates and recommends courses of action and response strategies. Designated agency representatives include the IOT Chief Information

Security Officer, or designee, ISP Commander, Intelligence and Investigative Technologies or designee, INNG Defensive Cybersecurity Programs Lead, or designee, Indiana Cybersecurity Program Director, IDHS Division Director, Response and Recovery, or designee and selected subject-matter experts.

## FEDERAL AGENCIES

### U.S. DEPARTMENT OF HOMELAND SECURITY

The Department of Homeland Security (DHS) is the designated lead agency during a cybersecurity incident requiring a federal response. Their primary functions are to identify the source of disruption and help remove it, determine how they gained access, assess the damage, and provide guidance to the organization on how to make their system more secure.

### FEDERAL BUREAU OF INVESTIGATIONS

The FBI is the lead federal agency for investigating cybersecurity-attacks by criminals, overseas adversaries, and terrorists. Specially trained FBI agents and analysts based at the FBI Indianapolis Field Office investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud.

### U.S. SECRET SERVICE

The Secret Service maintains Electronic Crimes Task Forces, which focus on identifying and locating international cybersecurity criminals connected to cybersecurity intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cybersecurity training and information to combat cybersecurity crime.

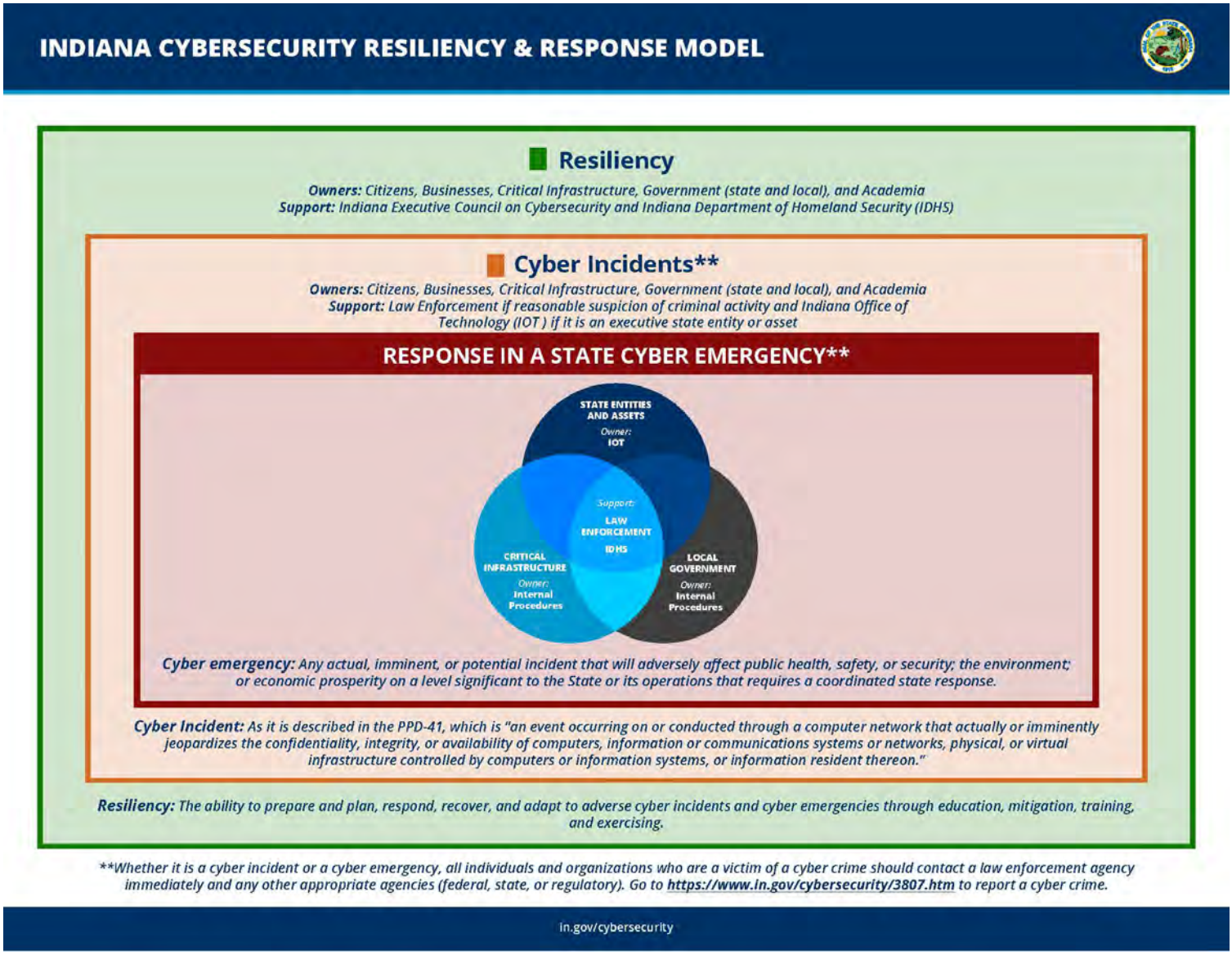
### U.S. DEPARTMENT OF JUSTICE

DOJ's Offices of U.S. Attorneys and its' Criminal and National Security Divisions, working with federal law enforcement agencies, use criminal and national security authorities to investigate, prosecute, and disrupt cyber threats and to apprehend cyber threat actors. Information and evidence obtained pursuant to appropriate legal process are used to identify the source of cyber incidents and to gather pertinent cyber threat information.

## 5.0 Cyber Emergency Resiliency Efforts

The State of Indiana core agency group include the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana National Guard, and Indiana State Police.

This core agency group assists and leads in the overseeing of the cybersecurity resiliency efforts of the Indiana Executive Council on Cybersecurity and the ability for the state to be prepared to enable the rapid and effective response needed by state government constituents during a cyber emergency or cyber incident as appropriate. The following Indiana Cybersecurity Resiliency and Response Model further identifies the owners and support organizations during the resiliency phase, a cyber incident, and a cyber emergency.



## 6.0 Response Process

### Report a Cyber Crime

When an organization's experiencing a cyber attack, the following these steps should be taken.

Step 1: Contact Law Enforcement

- FBI Internet Crime Complaint Center (IC3)
- Indiana State Police (ISP) Cybercrime and Investigative Technologies
- If there is an immediate threat to public health or safety, call 911.

Step 2: Additional Reporting

In addition to reporting the cyber attack, an organization should consider contacting other agencies to report the attack, which include:

- **Indiana Attorney General** requires organizations report any security breach resulted in exposure of personal information. For more information, click here.
- **Regulators:** Regulated organizations may need to report cyber crimes to other state or federal agencies.
- **Secretary of State:** If necessary, contact the SOS offices regarding any related cyber incidents at electionsecurity@sos.in.gov
- **Federal Government:** This fact sheet explains how to report cyber crimes to many federal agencies.
- **Indiana Department of Homeland Security** at WatchDesk@dhs.IN.gov.

Step 3: Utilize additional resources

For additional tips regarding avoiding ransomware and information from the National Governors Association Response Planning Memo, National Emergency Readiness Team information, Department of Homeland Security's National Cybersecurity and Communications Integration Center, and more visit www.in.gov/cybersecurity/3807.htm.

Step 4: Information Sharing

It's important to share cyber crime information with other organizations to protect critical infrastructure, the State of Indiana, and our nation. Learn more at www.in.gov/cybersecurity/3819.htm.

It is important to note that once the State of Indiana is notified, the following process was created with a single objective: Get the emergency into the hands of capable, representative, and empowered individuals to bring Indiana government resources and relationships quickly to the aid of those suffering from a cyber emergency.

Once a request for assistance is received by one or more state agencies, the core agency group will convene and assess the traits and impacts of the cyber incident or emergency and the value of their resources as they apply to an effective response to the emergency, whether it is with state resources or working with other key public and private partners. Cyberattacks shared with the State of Indiana will stay at the highest level of leadership and only shared with need-to-know parties. After each cyber event reported to one or more of the core agency group, a post-emergency evaluation will be completed by the state's Cybersecurity Program Director to rate response effectiveness, identify additional needs, and process adjustments.

## 7.0 Plan Maintenance

The State of Indiana Department of Homeland Security Executive Director, Indiana Office of Technology Chief Information Officer (CIO), and Indiana Cybersecurity Program Director are responsible for overall administration and maintenance of this State Guide.

# Integrated Preparedness Information Handout

# INTEGRATED PREPAREDNESS CYCLE

The Integrated Preparedness Cycle of planning, organizing/equipping, training, exercising (POETE), and evaluating/improving is a continuous process that ensures the regular examination of ever-changing threats, hazards, and risks, as shown in Figure 2.1.


**Figure 2.1: The Integrated Preparedness Cycle**

The Cycle involves the assessment of threats, hazards, and risks; new and updated plans; and improvements implemented from previously identified shortfalls or gaps.

Effective program management is comprised of the following components: •Engaging senior leaders; •Establishing multi-year preparedness priorities; •Conducting an Integrated Preparedness Planning Workshop (IPPW); •Developing a multi-year Integrated Preparedness Plan (IPP) and Integrated Preparedness Schedule (IPS); •Maintaining program reporting of exercise outcomes; and •Managing exercise program resources.

## INTEGRATED PREPAREDNESS PLANNING WORKSHOP (IPPW)

### PURPOSE

Use guidance provided by senior leaders to identify and set preparedness priorities and develop a multi-year schedule of preparedness activities.

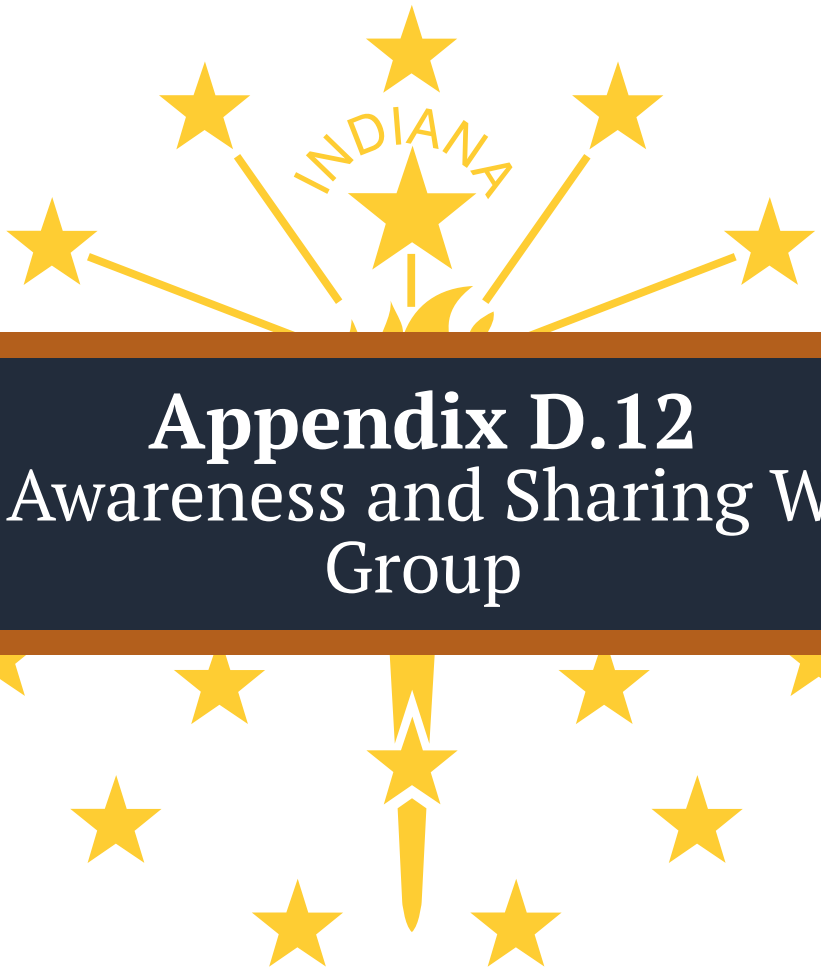
The process confirms: •Coordination of whole community initiatives; •Prevention of duplication of efforts; •Assurance of the efficient use of resources and funding; and •Avoidance of overextending key agencies and personnel.

During the IPPW, participation from the whole community ensures preparedness activities are included in the program's priorities.

CONTACT INFORMATION •Exercise@dhs.IN.gov•

### WORKS CITED

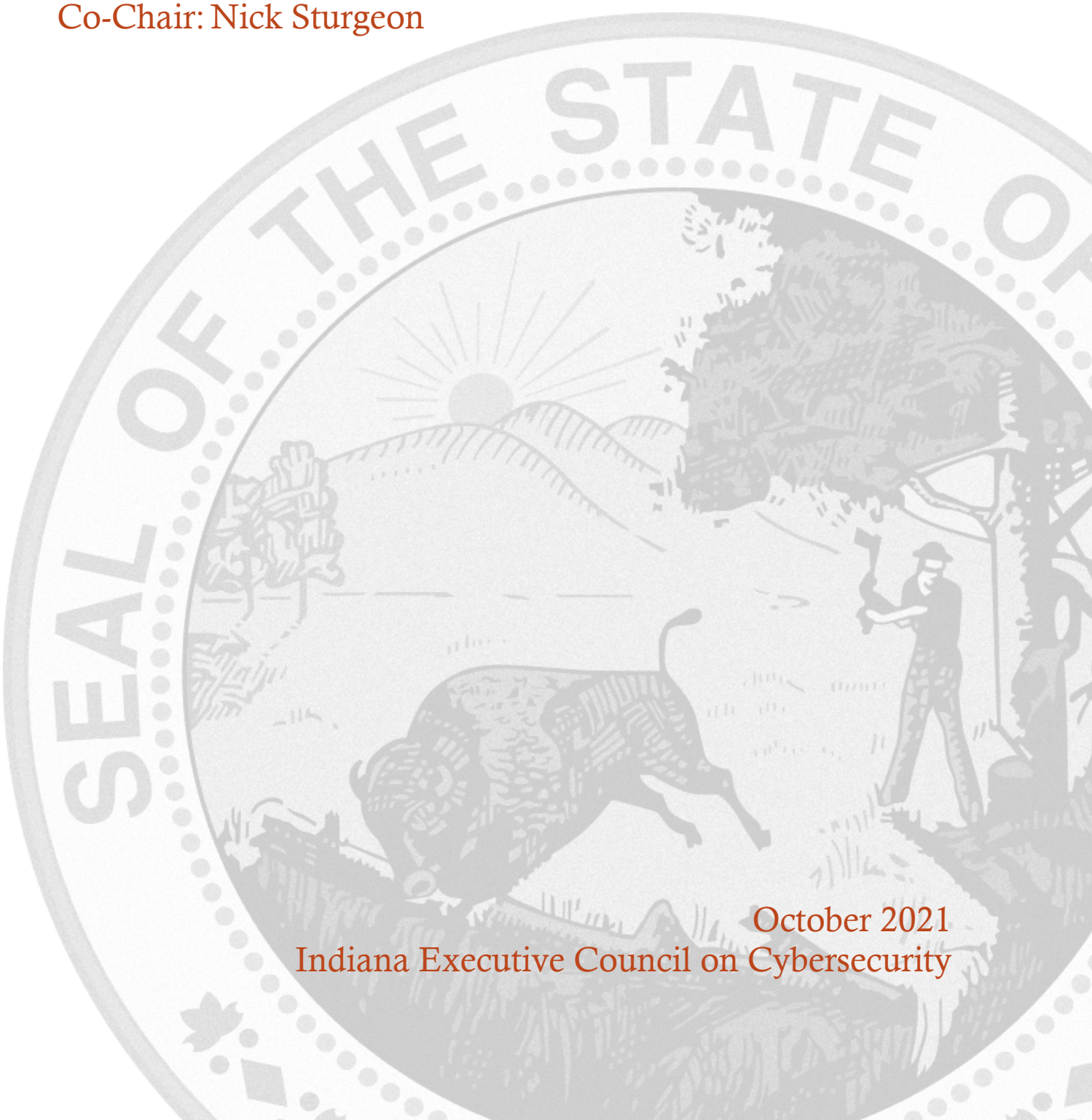
Homeland Security. "Homeland Security Exercise and Evaluation Program (HSEEP) January 2020." www.fema.gov/sites/default/files/2020-04/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf.




# Appendix D.12
## Cyber Awareness and Sharing Working Group

# CYBER AWARENESS AND SHARING WORKING GROUP STRATEGIC PLAN

Chair: Tracy Barnes
Co-Chair: Nick Sturgeon




October 2021
Indiana Executive Council on Cybersecurity

# Cyber Awareness and Sharing Working Group Strategic Plan

# Table of Contents

# Committee Members

## Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Adenike O. | Adetola | 360 Security United | SOC | As Needed |
| Akgul | Arif | Indiana State University | Assistant Professor School of Criminology & Security Studies | As Needed |
| Ayers | David | Indiana Office of Technology | Program Communications Manager | Chair Proxy |
| Barnes | Tracy | Indiana Office of Technology | Chief Information Officer | Chair |
| Braidich | Richard | RCR Technology | Chief Information Security & Privacy Officer | As Needed |
| Bush | Ron | Ron Bush Consulting, Inc. | President | As Needed |
| Cerny | Kirk | Haystax, A Fishtech Group Company | Senior Director | As Needed |
| Davis | Philip | Community Health Network | Director, IT Risk and Compliance | As Needed |
| Ferrante | Anthony | FTI Consulting | Global Head of Cybersecurity, Senior Managing Director | As Needed |
| Giles | Clark | City of Indianapolis | Chief Technical Officer | Full Time |
| Harmon | Tim | Journalist | Journalist | Full Time |
| Hosick | David | Indiana Department of Homeland Security | Communications Director | Full Time |
| Jackson | Craig | IU Center for Applied Cybersecurity Research | Program Director | As Needed |

| | | | | |
|---|---|---|---|---|
| Jirik | Jiri | Ivy Tech Community College | Assistant Professor - Evansville | As Needed |
| Johns | Jason | Sondhi Solutions | President | As Needed |
| Johnston | Kathleen | Michael I. Arnolt Center for Investigative Journalism, Indiana University | Founding Director | As Needed |
| Keller | John (Dr.) | Indiana Department of Education | Chief Information Officer, IT | As Needed |
| Lodin | Steve | Sallie Mae Bank | Senior Director, Cybersecurity Operations | As Needed |
| Lohrentz | John | Munster Police Department | Intelligence Analyst / Digital Forensic Analyst | Full Time |
| Lubsen | Graig | Indiana Office of Technology | Director of Communications | Full Time |
| McGraw | Michael | McGraw Consulting Group LLC | Senior Consultant | As Needed |
| Meadors | Joe | Gaylor Electric Inc | Vice President of Information Services | As Needed |
| Merkner | Karl | United Federal Credit Union | Security Engineer | As Needed |
| Ndow | Emmanuel | Marion General Hospital | Chief Information Officer | As Needed |
| O'Hara | Brian | BTO Associates, LLC | President/CEO | Full Time |
| Pirau | Ron | Archdiocese of Indianapolis | Chief Information Officer | As Needed |
| Potchanant | Joe | Indiana University - REN-ISAC | Director of Member Services and Support | Full Time |
| Rogers | Marcus | Purdue Polytechnic | Professor/Executive Director Cybersecurity Programs/Chief Scientist HTCU | As Needed |
| Ross | Michael | Indiana Criminal Justice Institute | Behavioral Health Division Director | Full Time |

| | | | | |
|---|---|---|---|---|
| Scarbro Kennedy | Valinda | IBM | IBM Global University Specialty Programs Manager-Medical, Legal, and HBCUs | Full Time |
| Schmelz | Pam | Ivy Tech Community College | Chair, School of Information Technology | Full Time |
| Schroers | Steven | Winston and Strawn, LLP | Technical Support Supervisor | As Needed |
| Stahl | Tad | IN-ISAC / Indiana Intelligence Fusion Center | Director / Deputy Director for Cyber Intelligence | Full Time |
| Sturgeon | Nick | IU Health | Director, Information Security | Co-Chair |
| Vuppalanchi | Deepika | Syra Health | CEO | As Needed |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

# Executive Summary

# Executive Summary

- **Research Conducted**
  - State cybersecurity plans
  - Magazine articles on state cyber sharing and cyber education
  - Team member familiarity with resources and professional techniques
  - Applied experience by team members for their own operations, experience, and networks with other organizations

- **Research Findings**
  - An inventory of cyber sharing resources and cyber education/awareness from various sources
  - Articles depicting the various strategies used by state governments
  - Best practices from other industries in education and training
  - 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)

- **Additional Notes**
  - No Response

- **References**
  - State cybersecurity plans (multiple)
  - $(ISC)^2$ Cyber Edge Group 2021 Cyberthreat Defense Report
    Pew article - http://pellcener.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf
  - $(ISC)^2$ 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

- **2021 Working Group Deliverables**
  - Public Relations Campaign Plan
  - Inventory of Cyber Sharing Resources
  - MS-ISAC Member Recruitment
  - Best Practices
  - Cyber Sharing Maturity Model
  - Sharing Community Slack Channel

# Research

# Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. There has been limited 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.
    b. Over the last few years, the efforts of the IECC have included managing a website called the Indiana Cyber Hub (www.in.gov/cybersecurity) using the resources and subject matter expertise of the more than 200 members of the Council.
    c. In addition to the website, the IECC team along with many Council members are regular contributors to the Indiana Cyber Blog that the public can subscribe to if they would like to receive interests.
    d. Along with the website, the Indiana Cyber Hub and its cyber awareness and education efforts has included social media presence on Twitter and Facebook.
    e. Over the last several years, there continues to be an emerging number of excellent cyber sharing resources. The process of finding information can be initially difficult and sometimes 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.
    f. Different sources of information take various approaches to distribute material to their audiences. These approaches include:

        - Corporate sources as a primary product
        - Technical sources as an enhanced support
        - Information Sharing and Analysis Centers (ISAC) serving particular sectors against common threats
        - 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. The greatest vulnerability is the general lack of both awareness and knowledge among the general public on how best to protect themselves from cyberattacks.
    b. It can also be challenging to filter 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.
    c. Many agencies and organizations 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. Public knowledge gap
    b. To identify needs to be facilitated by the Council and filled to scale.
    c. 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. While Indiana led the way in developing a statewide communication plan, other states have developed and fully implemented a cybersecurity education plan since 2018. Virginia was used as an initial model. Michigan provides local governments and organizations information and has a phone app with cybersecurity awareness and education. Colorado National Cybersecurity Center has partnered with Google to implement a national campaign with state officials and legislators on cyber education.
    b. Most states find themselves in a similar position as Indiana when it comes to cyber sharing. Fusion Centers may be the most common form of information distribution at a criminal level, but are limited in audience and specific in 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. Please collect and document.**
    a. $(ISC)^2$ Cyber Edge Group 2021 Cyberthreat Defense Report
    b. State of Cybersecurity Report 2020 I Accenture
    c. https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html
    d. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdfx

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Governors' Association and selected (few) states. Individual Indiana state agencies with limited perspectives and individually focused activities.
    b. Many states have looked to 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. Over the next 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.
    b. Identify 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.
    c. Success will also 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. While the State of Indiana has most certainly increased its number of resources in cyber security education within the state agencies as well as public, there could be opportunities for general cyber information to broad audiences/communications or specific information/communications for narrower audiences.
    b. 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. No Response

11. **What do we need to do to attract cyber companies to Indiana?**
    a. A vibrant and energetic cyber community, complete with sharing and cyber education 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. Over the last several years, through its development of the Indiana Cyber Annex with the Indiana Department of Homeland Security, there have been good discussion and processes put in place to best communication and assist those in need during a cyber emergency. Additionally, like other hazards, we would lean on the current procedures for Indiana Joint Operations Center and Joint Information Center for public awareness of a cyber emergency.
    b. Additional organizational communication protocols may vary with each organization, especially with sharing cyber security information. However, 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. 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: Public Relations Campaign Plan

# Deliverable: Public Relations Campaign Plan - Update

## *General information*

1. **What is the deliverable?**
    a. Update to the 2018 Public Relations Campaign Plan that will include more of a phased approach to further increase the public awareness, knowledge, and application of positive cybersecurity behaviors by all Hoosiers. The plan is also intended to promote cybersecurity as a career field and inform and educate the public about the activities of the Indiana Executive Council on Cybersecurity (IECC).

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?**
    a. As of August 2021, the initial activation of the plan is in place, with the execution of an ongoing communications program; participating in the "Days of Our Cyber Lives" podcast series; completion of significant updates to the Indiana Cyber Hub website, established presence on social media (on Twitter and Facebook – Sept. 2020) formal launch of the Indiana Cyber Blog (Dec. 2020) as a foundation for achieving the deliverable.

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?**
    ☒ 2021 ☐ 2022 ☐ 2023 ☒ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. All Hoosiers

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. While there are state departments promoting good cybersecurity habits, research suggest a continuing need to increase statewide coordination and a holistic approach to the problem.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The state of Indiana will be working with all other committees and working groups for assistance, as needed, for targeting behaviors of employees and businesses, industry, and trade groups, as well as those involving education (Pre-K-16+).

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 – partnering with CISA, USDHS as a resource for best practices
    b. State agencies: IOT, Department of Homeland Security (DHS) along with the Governor's office
    c. Associations: Selected industry and trade associations, through partnerships that exist statewide, including those whose work involving the IECC and its members

12. **Who should be main lead of this deliverable?**
    a. Program Communications Manager with IOT, at the direction of the Cybersecurity Program Director for the State of Indiana.

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

a. Implementation of some aspects of the plan will require funding and/or additional resources.

## *Implementation Plan*

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

☐ One-time deliverable

☒ Ongoing/sustained effort

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Initial PR Plan Developed | IECC Working Group | 100% | May 2018 | |
| Review of PR Plan and reworked for current resources and budget constraints | IECC Communication Program Manager | 100% | March 2020 | |
| Review of PR Plan | IECC Communication Program Manager and IECC Working Group | 75% | November 2021 | |
| Approval of Update to PR Plan | IECC Program Director and IECC Working Group | 0% | December 2021 | |
| Activation of Plan | IECC Partners with the IECC Communication Program Manager leading and tracking the efforts | 25% | January 2022 | Be sure to share final plan with working group |
| Review measurable successes of outputs and outcomes of PR Plan | IECC Program Director and IECC Communication Program Manager | 0% | December 2022 | Present to working group |
| Repeat above steps every year to keep the plan refreshed and considerate of time and resources | IECC Partners with IECC Communication Program Manager leading and IECC Program Director tracking the efforts | 0% | 2022-2024 | |

## 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 |
|---|---|---|---|---|---|
| At least one | At least one | Program Communications Manager | Appropriated | None | The Program Communications Manager is a very experienced public relations professional working at the direction of the Cybersecurity Program Director and whose overall responsibility is defined as plan execution, public representation, and coordination among key agencies. Will also oversee activities and budget for additional resources, up/to including the participation of an advertising agency, purchase of external resources/services related to analytics, media monitoring, as defined/needed to provide measurement of the outcomes, as defined in the deliverable. |

**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 | TBD | TBD | State | Private Sector and/or grant from federal government | |
| Purchase of advertising space | Support of campaign; broad reach; message consistency | Incl. | Incl. | TBD | TBD | |

## 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, 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.
b. In the absence of available funding, there is a potential cost to individuals and businesses related to a cyberattack or a data breach, the average cost of which, according to a recent report from IBM, is $4.62 million and $4.24 million, respectively.

**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. Additionally, educational opportunities could be lost, in the absence of encouraging people, especially middle school, high school and college students, from pursuing a career in cybersecurity. A loss in momentum and capitalizing on the progress achieved through the establishment of and the ongoing work of the IECC as a model for cybersecurity governance and its position at the forefront nationally among other state governments.

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

a. An acceptable return on investment (ROI) for a marketing campaign is, typically, a ratio of 5-to-1 in the way favorable media coverage and/or exposure with the intended audience(s) compared to the budget. An exceptional ROI is considered to be in the range of 10-to-1. There are 10 methods that can be used to help define the metrics to use as a 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?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. Every state. But, not recommended.
b. We can examine using Ohio or Illinois or Kentucky. The challenge will be conducting sufficient research to measure their lack of activity and results.
c. In this case, it is more important to measure against a national standard (i.e., Pew Study, updated additional resources/methods) 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 (i.e., Advertising Agency and state staff support)

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

☒No ☐ Yes

**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. Working with the Program Communications Manager and Cybersecurity Program Director.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. Statewide with all Hoosiers, as well as by the public and private sectors (all businesses/industries, organizations, non-profits, education).

## Communications

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

a. IECC
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)?**

☒No ☒ Yes

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

a. No Response

## *Evaluation Methodology*

**Objective 1:** The IECC Communications Program Manager will use the 2018 Statewide PR Cybersecurity Campaign Plan and develop a phased approach to the tactics as resources allow by December 2021.

*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 Communications Program Manager will leverage the assets of Indiana's cybersecurity program to create an increasingly larger presence on social media channels including Twitter, Facebook, and LinkedIn increasing its subscription by 30% each fiscal year.

*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:** The IECC Communications Program Manager will update a weekly blog as a tool for measurably increasing public awareness by further positioning Indiana as a leader in cybersecurity and increasing its subscription by 25% each fiscal year.

*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 - Update

## *General Information*

1. **What is the deliverable?**
    a. An update to the 2018 inventory of resources assembled by the IECC

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?**
    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. 2021

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. 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. Not applicable

12. **Who should be main lead of this deliverable?**
    a. Cyber Awareness and Sharing Working Group with the lead being IN-ISAC

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?**

☐ One-time deliverable
☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| List developed | IN-ISAC Manager | 100% | July 2021 | Ongoing only in those additional resources can be added |
| | | | | |
| | | | | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| 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?**

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 are the estimated costs associated with that risk reduction?**

a. The deliverable 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. One 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?**

☐No ☒ Yes

a. 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. 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. No Response

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, all sectors.

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 Awareness and Sharing Working Group will complete an inventory of cyber sharing resources by August 2021.

*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?**
    ☐ 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?**
    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?**
   ☒ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

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, IN-ISAC manager

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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review Outreach plan | IN-ISAC Manager | 100% | February 2021 | |
| Implement plan and tactics | IN-ISAC Manager | 50% | December 2021 | |
| Update outreach plan and implement | IN-ISAC Manager | 0% | 2022-2024 | To be done annually |

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1.0 | N/A | IN-ISAC manager | State Indiana Office of Technology | 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?**

☐No ☒ Yes

a. 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?**

☒No ☐ Yes

**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. IN-ISAC

**27. Can this deliverable be used by other sectors?**

☒No ☐ Yes

a. Local governments 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)?**

☐No ☒ Yes

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

a. None as of now.

## *Evaluation Methodology*

**Objective 1:** Indiana-ISAC will work to increase MS-ISAC membership by 25 percent each calendar year.

*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 Best Practices

# Deliverable: Cyber Sharing Best Practices - Update

## *General Information*

1. **What is the deliverable?**
    a. Provide an updated list of cyber sharing best practices

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?**
    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?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. USDHS CISA practices and guides with additional resources that may 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?**
    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 Awareness and 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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review List developed in 2018 | Nick Sturgeon | 75% | March 2022 | |
| Review with the Working Group | Cyber Sharing Working Group | 0% | May 2022 | |
| Present update on the deliverable | IECC | 0% | June 2022 | |
| Post on Cyber Hub website | IECC Communications Manager | 0% | July 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| 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 are 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. While updating this deliverable will only cost time to make the updates to the Indiana Cybersecurity website, an organization could lose time and money if they are unaware of a best practice and undergo a cyberattack as a result. Many look to the state for key education on protecting themselves and businesses. So, developing this and people using it may create a needed efficiency and prevent an organization from a cyberattack.

**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?**

☐No ☒ Yes

**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?**

☐No ☒ Yes

## 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?**

☒No ☐ Yes

**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. The only people contacted to this point are those within the Cyber Awareness and Sharing Working Group.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. All Sectors

## 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)?**

☐No ☒ 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 Awareness and Sharing Working Group will update a list of best practices by July 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 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?**
    ☐ 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?**
    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?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. 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. 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. No Response

12. **Who should be main lead of this deliverable?**
    a. Cyber Awareness and Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Quantifying success of the model and keeping it simple enough for all to use.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Rework 2019 Draft of model | Cybersecurity Program Director | 100% | March 2020 | |
| Review and develop model | Cyber Awareness and Sharing Working Group, Strategic Resources Working Group | 50% | February 2022 | |
| Present model for feedback from Council | IECC | 0% | April 2022 | |
| Make edits and design | Cybersecurity Program Director and Cyber Sharing Working Group | 0% | May 2022 | |
| Finalize Model | Cyber Sharing Working Group | 0% | June 2022 | |
| Incorporate model into IECC PR and Communications Plan | Public Awareness and Training Working Group | 0% | July 2022 | |
| Distribute to stakeholders | IECC and partners | 0% | August 2022 | |

## 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 |
|---|---|---|---|---|---|---|
| No Response | | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

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 are 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. Due to the confusion, 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. The users 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?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. 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?**

☒No ☐ Yes

**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. 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?**

☐No ☒ Yes

a. All Sectors

## 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)?**

☐No ☒ 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 Awareness and Sharing Working Group will edit and post the Indiana's updated cyber sharing maturity model by July 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

**Objective 2:** IECC Cyber Awareness and Sharing Working Group will distribute Indiana's updated cyber sharing maturity model to critical infrastructures through ninety percent of Indiana associations by August 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 Sharing Community Slack Channel

# Deliverable: Cyber Sharing Community Slack Channel

## *General Information*

1. **What is the deliverable?**
   a. Launch a Cyber Sharing Community Slack Channel

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?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices
   ☒ 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 facility a grass roots level sharing of cybersecurity information (i.e. Indicators of Compromise (IOCs), cyber observables, threats, intelligence, tactics, techniques, and procedures) among the IECC members at a tactical/technical level.

6. **What metric or measurement will be used to define success?**
   - Number of IECC members in the IECC Cyber Sharing Community Slack
   - Channel Number of IECC members engaged in the Slack Channel.
   - Total messages in the Slack Channel.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. All IECC Members and their organizations

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

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Healthcare 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. We will need representation from as many IECC Working Groups and members to get the most out of the effort.

12. **Who should be main lead of this deliverable?**
    a. Nick Sturgeon, Co-chair of IECC Cyber Awareness and Sharing Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Getting the IECC Members to actively participate in the Slack Channel.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Set up the Channel | Nick Sturgeon | 100 | May 31, 2021 | |
| Beta Test | Nick Sturgeon | 50% | November 30, 2021 | |
| Go Live | Nick Sturgeon | 0% | January 31, 2021 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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 |
|---|---|---|---|---|---|---|
| Slack Channel | This application is the medium in which the sharing will take place. | Free | $8/person | No Response | No Response | To get additional capabilities and features from the slack channel we would need to move up to the Pro plan. |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. The IECC Cyber Sharing Community Slack Channel will provide a medium in which the technical cyber security staff of our members can sharing cyber information in real time.

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

a. This Slack Channel will provide the means in which our member organizations and their cyber security/IT staff share cyber information in real time. This allows them to connect with their peers in other organizations at a level they determine is sufficient. This also removes a choke point in sharing information by eliminating the need to rely on one person to distribute information. Additionally, individuals can determine what information to share and what information to consume. The biggest cost reduction is time.

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

a. That critical cyber information will not get shared as broadly as needed.

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

a. The definition of success will be the total participation and engagement of the IECC members.

**21. 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

**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?**

☒No ☐ Yes

## 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?**

☒No ☐ Yes

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

a. We will need engagement from the IECC member organizations to keep this going.

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

a. IECC Healthcare Committee

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

## Communications

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

a. The IECC members

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

☒No ☐ Yes

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

a. Communication to IECC members via the IECC leadership.

## *Evaluation Methodology*

**Objective 1:** IECC Cyber Awareness and Sharing Working Group will create the Slack Channel by May 2021.

☐ 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 Awareness and Sharing Working Group and IECC Healthcare Committee will conduct a beta test of the Slack Channel by December 2021.

☒ 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:** Complete the Live Production Launch of the Slack Channel by January 2022.

☐ 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 the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

a. 2018 Public Relations Plan
b. Cyber Sharing Resources Inventory 2021
c. Cyber Maturity Model Draft

# 2018 Public Relations Plan


# Indiana Executive Council on Cybersecurity

# Public Awareness and Training Plan

# 2018-2020

**Public Awareness and Training Working Group**

June 2018

**TABLE OF CONTENTS**

## 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

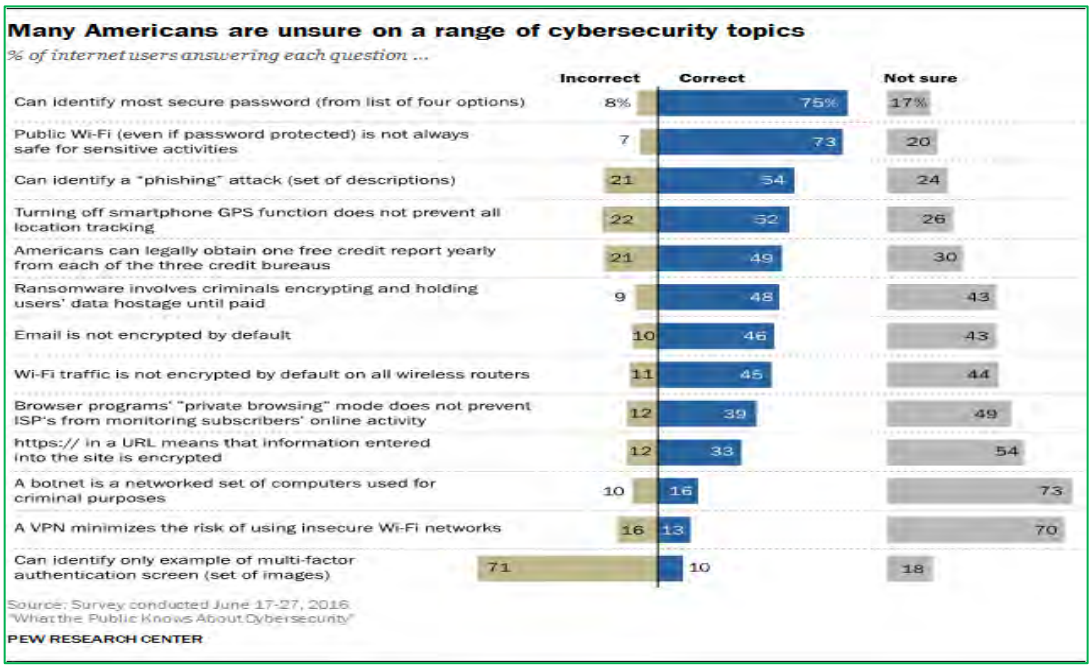
Summary

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

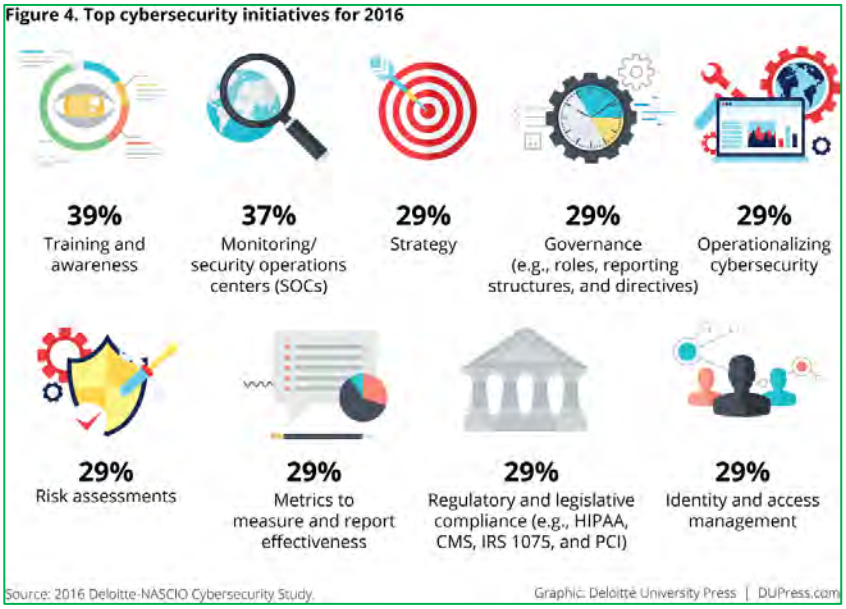
    b. Some key facts from the report:
        - The world economic forum's global risks 2015 report highlighted cyberattacks and threats as one of the most likely high-impact risks. In the United States, for example, cybercrime already costs an estimated $100 billion a year.
        - IOT Sensors and devices 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<br><br>$1,500<br><br>$10,000<br><br><u>Total</u>: $143,000 | Initial campaign development<br><br>Monthly creative<br><br>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.<br><br><u>Alternative</u>: hire entry level PR professional to manage. Use qualitied volunteers for speakers. | $0<br><br>$42,000<br><br>$12,000 | Development and maintenance.<br><br>Alt: PR Coordinator: $30,000 plus benefits.<br><u>Note</u>: 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.<br><br>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<br>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. |

# Cyber Sharing Resources Inventory 2021

# 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/public-resources/AlertsAdvisories.html |
| | Open DNS | | | | https://www.opendns.com/ |
| | H-ISAC | | | | https://h-isac.org/threat-intelligence/ |
| Advisories | FinCEN (Financial Crimes Enforement Network) | | | | https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets/advisories |
| | 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 Counci | | 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/ |

# Cyber Maturity Model Draft

# Cyber Sharing Maturity Model
## DRAFT

| Level | Maturity | Score | Resources for Model – INSERT MATURITY RESOURCE LINKS TO IMPROVE SCORE & LEVEL |
|---|---|---|---|
| 5 | Intake information shared by cyber sharing networks | 3 – Optimizing:<br>2 – Progressing:<br>1 – Limited:<br>0 – Not Started | • ISAO Standards Organization: *ISAO 300-1 Introduction to Information Sharing*, Section 3.2 Applying Shared Information<br>• ISAO Standards Organization: *ISAO 300-1 Introduction to Information Sharing*, Figure 3. Applying Information to Cybersecurity Risks<br>• DHS Cyber Information Sharing and Collaboration Program (CISCP)<br>• Multi-State Information Sharing & Analysis Center<br>• Infrastructure Protection Gateway (IP Gateway):Vuln assessments & Data Analytics<br>• **The Office of Cyber and Infrastructure Analysis (OCIA)** provides infrastructure consequence analysis and prioritization capabilities. |
| 4 | Join cyber sharing networks | 3 – Optimizing:<br>2 – Progressing:<br>1 – Limited:<br>0 – Not Started | • ISAO Standards Org - Information Sharing Groups (57 as of Apr 2018)<br>• DHS Cyber Information Sharing and Collaboration Program (CISCP)<br>• Multi-State Information Sharing & Analysis Center<br>• Infragard |

| | | | |
|---|---|---|---|
| | | | • Infrastructure Protection Gateway (IP Gateway):Vuln assessments & Data Analytics |
| 3 | Internal policies of cyber threat sharing, aware of cyber sharing networks | 3 – Optimizing:<br>2 – Progressing:<br>1 – Limited:<br>0 – Not Started | • National Preparedness Course Catalog<br>o AWR-177-W Information Risk Management<br>o AWR-353-W Using the Community Cyber Security Maturity Model (CCSMM) to Develop a Cyber Security Program<br>• Information Sharing and Analysis Organization Standards Organization<br>• Multi-State Information Sharing & Analysis Center<br>• DHS Cyber Information Sharing and Collaboration Program (CISCP) |
| 2 | Cyber threat detection and recognition | 3 – Optimizing:<br>2 – Progressing:<br>1 – Limited:<br>0 – Not Started | • IBM: Raise the Red Flag: Guidelines for Consuming and Verifying Indicators of Compromise - https://securityintelligence.com/raise-the-red-flag-guidelines-for-consuming-and-verifying-indicators-of-compromise/<br>• National Preparedness Course Catalog<br>o AWR-169-W Cyber Incident Analysis and Response<br>o AWR-177-W Information Risk Management<br>• US-CERT Alerts<br>• DHS Cyber Information Sharing and Collaboration Program (CISCP)<br>• DHS Enhanced Cybersecurity Services (ECS)<br>• Multi-State Information Sharing & Analysis Center |

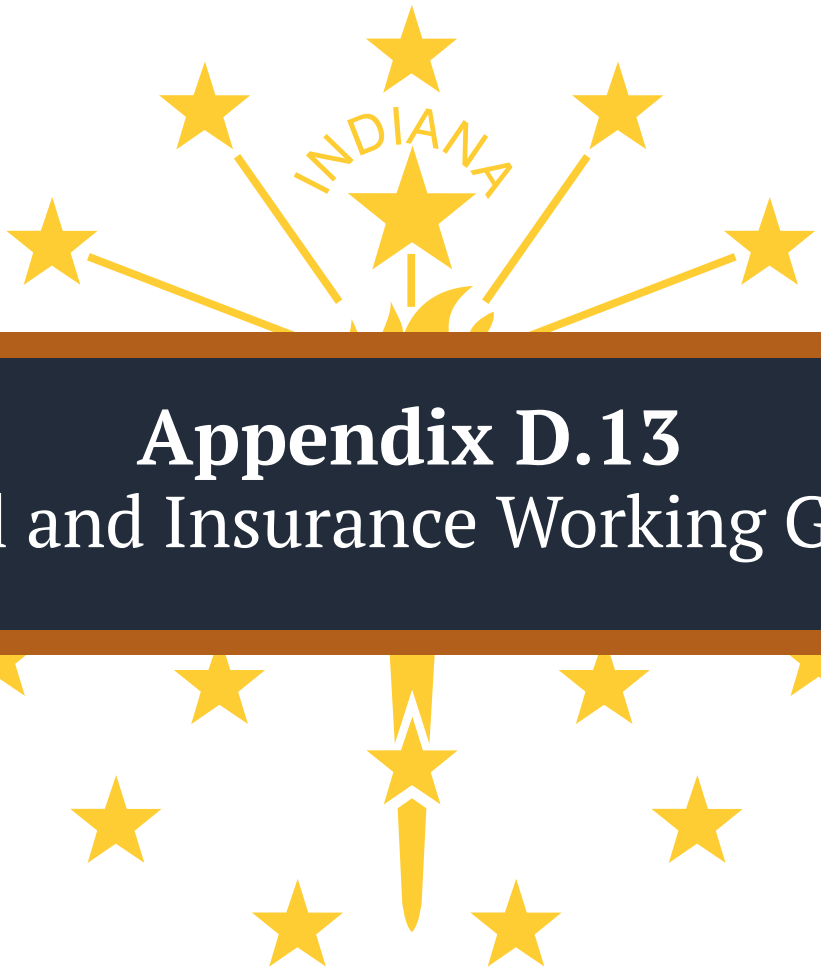
| | | | |
|---|---|---|---|
| | | | • Federal Virtual Training Environment (FedVTE) |
| 1 | Cyber threat awareness (prevention, protection, preparedness) | 3 – Optimizing:<br>2 – Progressing:<br>1 – Limited:<br>0 – Not Started | • US-CERT Nat'l Cybersecurity Awareness System Tips: https://www.us-cert.gov/ncas/tips<br>• DHS Cyber Information Sharing and Collaboration Program (CISCP)<br>• DHS Enhanced Cybersecurity Services (ECS)<br>• **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)**<br>• Multi-State Information Sharing & Analysis Center (MS-ISAC)<br>• National Cybersecurity Awareness Month (NCSAM)<br>• Federal Virtual Training Environment (FedVTE) |

**Definition of Maturity sublevels:**

**Limited** – Most basic level. For example, the organization may have limited processes, but does not have a clear policy and plan.

**Progressing** – Planning has begun and is in process.

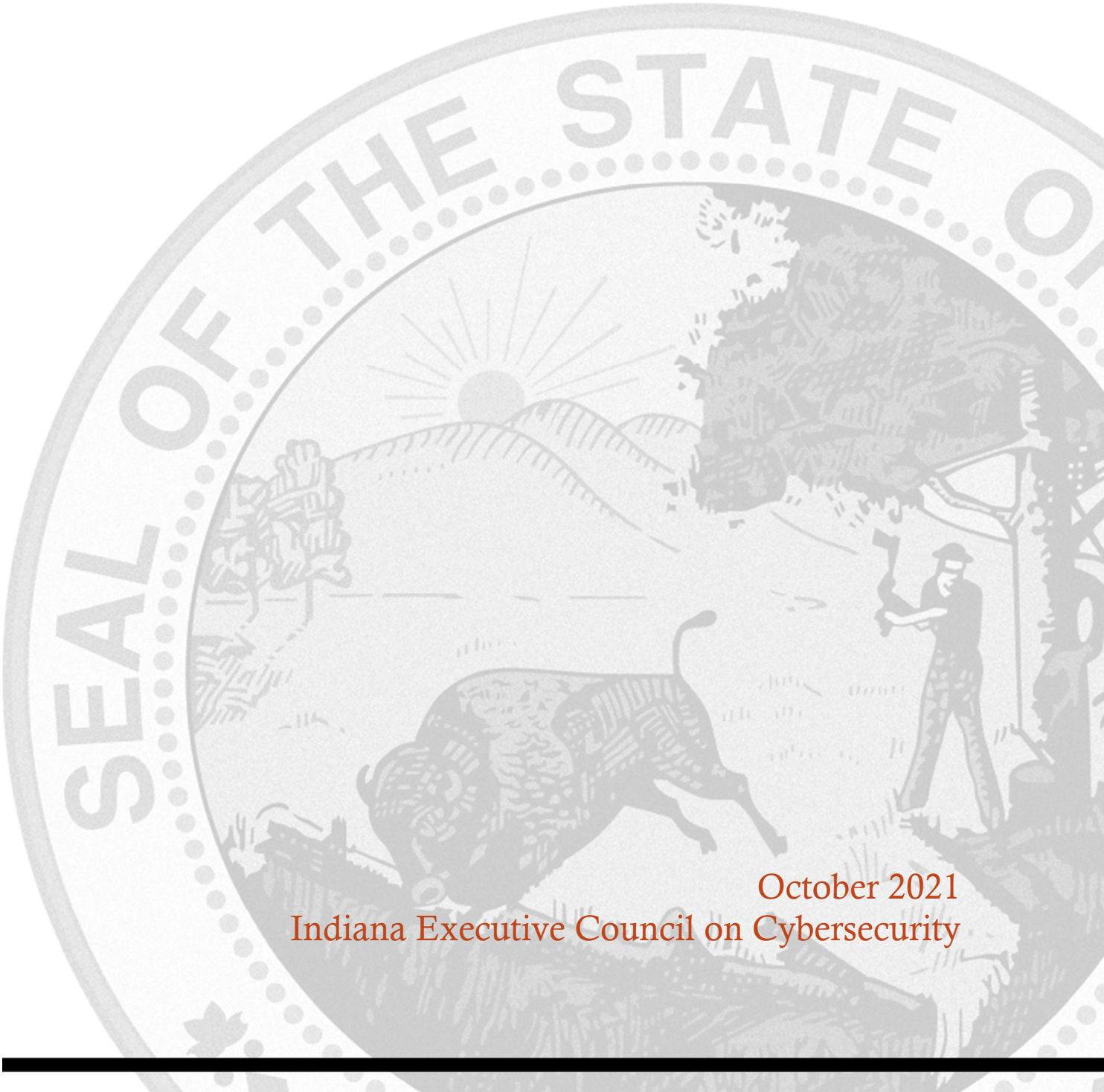
**Optimizing** – Highest level of maturity indicating that cyber sharing capabilities are fully developed and integrated into business processes. This includes automation tools.




# Appendix D.13
## Legal and Insurance Working Group

# LEGAL AND INSURANCE WORKING GROUP STRATEGIC PLAN

Chair: Todd Rokita
Co-Chair: Stephen Reynolds




October 2021
Indiana Executive Council on Cybersecurity

# Legal and Insurance Working Group Plan

# Table of Contents

# Committee Members

# Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Ehrenberg | Jim | Indiana Office of Technology | General Counsel | Full Time |
| Harper | Meredith | Eli Lilly and Company | Vice President, Chief Information Security Officer | Full Time |
| Howell | Michele | Aon Risk Services Central | Vice President, Business Development | Full Time |
| Ira | Adam | Frost Brown Todd | Attorney | Full Time |
| Putnam | Reid | Gregory & Appel Insurance | Vice President, Commercial Insurance | Full Time |
| Reynolds | Stephen | Baker McKenzie | Partner, IPTech | Co-Chair |
| Rokita | Todd | Indiana Attorney General | Attorney General | Chair |
| Souza | Diego | Cummins, Inc. | Global Chief Information Security Officer | Full Time |
| Swearingen | Mark | Hall, Render, Killian, Heath & Lyman, P.C. | Shareholder | Full Time |
| Swetnam | Douglas | Indiana Office of Attorney General | Section Chief – Data Privacy and Identity Theft Unit | Chair Proxy |
| Torres | Lori | Indiana Attorney General | Chief Deputy | As Needed |
| Vare | Todd | Barnes & Thornburg LLP | Partner | Full Time |
| Berry-Tayman, JD | Lisa | Kevel | Director of Security and Privacy | Full Time |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan.*

For more information, visit www.in.gov/cybersecurity.

# 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.

- **2021 Plan Working Group Deliverables**
  - Cyber Insurance Toolkit
  - Policy Review
  - Cyber Insurance Survey – Post-Covid
  - Funds Transfer Fraud Fact Sheet

- **Additional Notes**
  - None at this time

- **References**

# Research

# Research

**1) What has your area done in the last five years to educate, train, and prepare for cybersecurity?**

**INDIANA DEPARTMENT of INSURANCE**

a) There are now state laws governing cybersecurity breaches and reporting those breaches to the Indiana Department of Insurance. Indiana has enacted HB 1372 based on the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (MDL-668). The law requires state-regulated insurance entities to implement written information security programs, investigate and provide notification of cybersecurity events within a prescribed time, and maintain procedures for the secure disposal of nonpublic information.

b) As of July 1, 2021, Indiana law requires insurance companies and related entities in the insurance industry to report cybersecurity incidents and data breaches to the Indiana Department of Insurance.

i) HEA 1372 establishes a comprehensive regulatory framework requiring licensees to implement information security programs and report data breaches. HEA 1372 also empowers the Indiana Insurance Commissioner (IIC) to make related regulations and enforce the law.

ii) The law requires licensees to:

iii) Develop, implement, and maintain a comprehensive written information security program that:

iv) contains administrative, technical, and physical safeguards to protect nonpublic information;

v) is based on a risk assessment conducted by an employee, affiliate, or outside vendor;

vi) mitigates identified risks according to the licensee's size and complexity, the nature of its activities, and the sensitivity of the nonpublic information it controls; and

vii) defines and periodically reevaluates a retention schedule for nonpublic information and a procedure for its destruction when no longer needed.

viii) Establish a written incident response plan to promptly respond to and recover from cybersecurity events.

ix) Respond to a cybersecurity event by:

x) conducting a prompt investigation;

xi) performing or overseeing reasonable mitigation and restoration activities;

xii) notifying the IIC within three business days after determining that an event has occurred, under certain conditions; and

xiii) notifying affected consumers according to Indiana's consumer data breach notification law.

xiv) Notably, in contrast to the model law, HB 1372:

xv) Limits nonpublic information by excluding licensees' business-related information and focusing instead on consumers' personal data.

xvi) Does not include provisions regarding third-party service provider oversight or testing for externally developed applications.

xvii) Limits reportable cybersecurity events to those that have a reasonable likelihood of materially harming a consumer or any part of the licensee's normal operations.

xviii) Does not explicitly require program adjustments based on business or technical changes, and limits required program reporting to a licensee's executive management rather than its board of directors.

c) Offer and attending trainings both in person and virtually regarding how other state departments of insurance have handled cybersecurity breach notices.
d) Engaging in ongoing conversations with other state regulators with regards to cybersecurity enforcement and training.
e) The National Association of Insurance Commissioners (NAIC) formed an executive committee on cybersecurity and the IDOI/Indiana will serve as a committee member.
f) All cybersecurity insurance policies and rates offered by admitted insurers in the State of Indiana must first be filed with the Indiana Department of Insurance. The IDOI reviews the policy form and rate filings. Most commercial property and general liability policies do not cover cyber risks, and cyber insurance policies are highly customized for clients. In 2019, premiums were estimated at around $3.15 billion, a slight decrease of .22% from the prior year. This number reflects both stand-alone cybersecurity insurance products as well as those writing cybersecurity insurance as part of a package policy. The total Admitted Market for cybersecurity insurance coverage was about $2.03 billion and included both standalone and package policy coverage. The NAIC's notes that this amount represents a 6.81% increase over 2017 numbers.
g) The National Institute of Standards and Technology (NIST) has provided a framework for improving critical infrastructure cybersecurity. The framework provides a structure of standards, guidelines, and practices to aid organizations, regulators, and customers with critical infrastructures in effectively managing their cyber risks., most recently updated in 2018. The framework provides a structure of standards, guidelines, and practices to aid organizations, regulators and customers with critical infrastructures in effectively managing their cyber risks.
h) State insurance regulators serve on the U.S. Department of the Treasury's (Treasury Department) Financial Banking and Information Infrastructure Committee (FBIIC) where they work with federal regulators to address cyber threats in the United States. State insurance regulators continue to monitor cybersecurity in the insurance sector closely. In addition, regulators work with insurers to resolve immediate concerns when a data breach occurs at an insurance company. State insurance regulators are also in the unique position of regulating and monitoring the solvency and market activities of insurance carriers underwriting cybersecurity policies.
i) The IDOI led a national multi-state examination of Anthem following its data breach, which was the largest reported breach at the time, along with 49 states participating in the exam process.

**INSURANCE INDUSTRY**

a. Cyber Insurers and Brokers/Agents in the space have worked to educate the user-buyer community regarding the exposures, controls, and evolving landscape of Cyber Insurance through various forms. This has been an aggressively expanding and challenging area of Insurance so the marketing collateral and material publicly available is robust.
b. There have been numerous opportunities to educate and train on cybersecurity in the community through webinars, and training sessions that have been held. The IECC's cybersecurity guide that has resided on the state's cybersecurity hub, the Cybertech conferences that have been held in Indiana.

**INDIANA ATTORNEY GENERAL**

a. The Office of Indiana Attorney General worked with the Indiana State Chamber of Commerce to create a seminar on Cybersecurity
b. The Office of Indiana Attorney

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

**INDIANA DEPARTMENT of INSURANCE**

a) The reasons the financial services sector is susceptible to cyberthreats are multifaceted. Financial firms receive, maintain and store substantial amounts of personally identifiable information (PII); however, insurers, in many cases, receive personal health information in addition to personal financial information from both policyholders and claimants.
b) Healthcare breaches continue to grow each year. Research indicates that personal health information continues to be more valuable to hackers than other types of financial records, such as credit cards. Personal health information generally provides more information regarding PII than a financial record. A report authored by Trustwave suggests that a health care record may be worth up to $250 per record on the dark web; a credit card record holds a value of $5.40 per person, per card.

**INSURANCE INDUSTRY**

a. The biggest vulnerability continues to be under-educated user-buyers not leveraging Cyber Insurance as a piece/part of a robust overall Cyber Risk Management program. With the rapid changes occurring in the market, insureds can be underprepared for the Underwriting Requirements for certain Cyber controls, programs, and protocols necessary to procure good coverage.
b. Healthcare systems, small to middle-market companies that do not have the resources to implement controls, as well as municipalities and rural towns that lack resources.

**INDIANA ATTORNEY GENERAL**

a. IT vendors and cloud-based software as service providers who manage the transfer and storage of data.

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

**INDIANA DEPARTMENT of INSURANCE**

a) Additional training pertaining to how state departments of insurance handle cybersecurity breach notices.

**INSURANCE INDUSTRY**

a. Connecting technical Cyber Risk Management (Like from the IT or CISO's perspective) with the risk transfer of Cyber Insurance, so the decision makers are making an informed buying decision on Insurance aligned with their strategic growth objectives.
a. Continued education that cybersecurity is important to every size company.

**INDIANA ATTORNEY GENERAL**

a. Education/Outreach to local governments, schools, and small businesses

**4) To what federal, state, or local cyber regulations is your area beholden currently?**

**INDIANA DEPARTMENT OF INSURANCE**

a) Indiana Codes §§ 27-2-27-1 – 27-2-27-32 (Chapter 27, Insurance Data Security)
b) The Computer Fraud and Abuse Act ("CFAA") 18 U.S.C. § 1030
c) Electronic Communications Protection Act ("ECPA") 18 U.S.C. § 2702; 18 U.S.C. § 2511
d) The Gramm-Leach-Bliley Act
e) The NAIC Financial Examination Handbook, incorporated by reference into Indiana Code
f) HIPAA exemption allowed under Indiana Law IC § 27-2-27

**INDIANA ATTORNEY GENERAL**

a. Ind. Code §4-1-6 Fair Information Practices
b. Ind. Code §4-1-10 Release of Social Security Number
c. Ind. Code §4-1-11 Notice of Security Breach
d. Ind. Code § 5-14-1.5-1 et seq. IN Driver's Privacy Protection Act
e. Ind. Code § 4-13.1-2-9 – Cyber Incident Report
f. Health Insurance Portability and Accountability Act (HIPAA) of 1996
g. Genetic Information Nondiscrimination Act ("GINA") of 2008

<u>The Indiana Attorney General Enforces:</u>

a. Ind. Code §4-1-10 Release of Social Security Number
b. Ind. Code §4-1-11 Notice of Security Breach
c. Ind. Code §4-6-13-1 et seq. Abandoned Records
d. Ind. Code §24-4.7-1-1 et seq. Telephone Solicitation of Consumers
e. Ind. Code §24-5-0.5-1 et seq. Deceptive Consumer Sales Act
f. Ind. Code §24-5-12-1 et seq. Telephone Solicitations Registration
g. Ind. Code §24-5-14-1 et seq. Regulation of Automatic Dialing Machines (Rococall)

h. Ind. Code §24-5-14.5-1 et seq. False or Misleading Caller Identification (Spoofing)
i. Telephone Consumer Protection Act of 1991 (TCPA) 47 U.S.C. § 227
j. Federal Regulations on Telemarketing, Telephone Solicitation and Facsimile Advertising 47 CFR § 64.1200
k. Telemarketing and Consumer Fraud and Abuse Prevention Act 15 USC §6103(e)
l. Telemarketing Sales Rule 16 CFR § Part 310
m. CAN-SPAM Act 15 USC ch. 103
n. CAN-SPAM Rule 16 CFR Part 316
o. Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 USC §1320d
p. HIPAA Privacy, Security, Breach Notice and Enforcement rules 45 CFR parts 160, 162, 164

**INSURANCE INDUSTRY**

a. Understanding the various State Breach Statutes, and Federal Regulations and Compliance requirements that impact a given insured in a specific industry is critical incorporation to the structuring, selection of an appropriate Cyber Insurance program.

**5) What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**

**INDIANA DEPARTMENT of INSURANCE**

a) The IDOI has many resources and information developed both internally, from other states' departments of insurance, and from the NAIC.

**INSURANCE INDUSTRY**

a. Cyber Insurers and Agents/Brokers are constantly and consistently release Claim Scenarios documents and other material to inform the buying decisions.
b. There are many companies, such as AON, that have a very large cybersecurity practice, with a myriad of white papers available to publish and will continue to be thought leaders in the cybersecurity space.

**INDIANA ATTORNEY GENERAL**

a. White House memo from Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

**6) What research is out there to validate your group's preliminary deliverables**?

**INDIANA DEPARTMENT of INSURANCE**

a) The IDOI materials include studies from other states' departments of insurance, the federal government, and the NAIC.

**INSURANCE INDUSTRY**

a. No Response

**INDIANA ATTORNEY GENERAL**

a. State of Hoosier Cybersecurity 2020

**7) What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**

**INDIANA DEPARTMENT of INSURANCE**

a) Attending trainings both in person and virtually regarding how other state departments of insurance have handled cybersecurity breach notices.
b) Drafted a cybersecurity model law (#668) for states to use as a drafting model for their respective legislation.
c) There is now an NAIC executive committee on cybersecurity. Previously, several working groups under NAIC to discuss cybersecurity: Innovation and Technology (EX) Task Force and Cybersecurity (EX) Working Group
    i) These working groups have adopted:
    (1) Principles for Effective Cybersecurity: Insurance Regulatory Guidance. Attached here.
    (2) Roadmap for Cybersecurity Consumer Protections. Attached here.
    (3) Updated the Financial Condition Examiners Handbook for revised cybersecurity protocols.
    (4) Made recommendations to update the Market Regulation Handbook
d) NAIC membership adopted a Cybersecurity Insurance and Identity Theft Coverage Supplement for the property/casualty annual financial statement to collect information about cybersecurity insurance markets.
e) Cybersecurity risks should be incorporated and addressed as part of an insurer's or an insurance producer's enterprise risk management (ERM) process. Cybersecurity transcends the information technology department and must include all facets of an organization.

**INSURANCE INDUSTRY**

a. No Response

**INDIANA ATTORNEY GENERAL**

b. State Attorneys General have recommended businesses follow the minimum examples outlined in the Memo by Anne Neuberger on June 2, 2021.

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

**INDIANA DEPARTMENT of INSURANCE**

a) Following state and federal statutes with regards to enforcement and regulation of cybersecurity within the insurance industry.

**INSURANCE INDUSTRY**

a. Cyber Insurance should now be considered a Duty-of-Care coverage that any/all business should include in their Insurance portfolio – Hopefully by connecting the dots between prudent Cyber Security postures and appropriate Cyber Insurance programs, we can begin to turn the tide of Ransomware and associated Insurance claims (which then impact the cost and structure of the policies to the insured).
a. That, at a minimum, every organization would understand the importance of implementing MFA as a fundamental control. That there is knowledge around the importance of cyber insurance and what it covers and how it can help organizations in the face of a breach.

**INDIANA ATTORNEY GENERAL**

a. At least weekly outreach events to local governments, schools, and small businesses throughout Indiana to discuss cyber threats and steps to prevent and protect against cybercrime.

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

**INDIANA DEPARTMENT OF INSURANCE**

a) The IDOI will post on its website cybersecurity resources available to consumers and industry.

**INSURANCE INDUSTRY**

a. Should the state through the Indiana Department of Insurance (or various Insurance organizations like the Big I) push additional Cyber Insurance education/training CE requirements as part of the Bi-annual Insurance License renewal?

**INDIANA ATTORNEY GENERAL**

a. Understanding the ways in which personal information is misused to harm consumers, through identity theft, fraud, and unfair practices.

**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?**

**INDIANA DEPARTMENT of INSURANCE**

a) No Response

**INSURANCE INDUSTRY**

a. While the Insurance workforce in Indiana is robust, how much expertise/specialization in Cyber Insurance is undetermined.

**INDIANA ATTORNEY GENERAL**

a. No Response.

**11) What do we need to do to attract cyber companies to Indiana?**

**INDIANA DEPARTMENT of INSURANCE**

a) Consistency in regulation

**INSURANCE INDUSTRY**

a. No Response

**INDIANA ATTORNEY GENERAL**

a. Communications infrastructure.

**12) What are your communication protocols in a cyber emergency?**

**INDIANA DEPARTMENT of INSURANCE**

a) If there is a violation of Chapter 27 under Title 27, pursuant to Indiana Code § 27-2-27-27, the Commissioner may after notice and hearing suspend or revoke the license, certificate of authority, or registration of the licensee.

**INSURANCE INDUSTRY**

a. No Response

**INDIANA ATTORNEY GENERAL**

a. No Response

**13) What best practices should be used across the sectors in Indiana?**

**INDIANA DEPARTMENT of INSURANCE**

a) The cybersecurity financial examination and reporting requirements developed with the NAIC and implemented by state insurance departments could be adopted across sectors.

**INSURANCE INDUSTRY**

a. No Response

**INDIANA ATTORNEY GENERAL**

a. NIST Cybersecurity Framework

# Deliverable: Insurance Toolkit

# Deliverable: Insurance Toolkit

## *General Information*

1. **What is the deliverable?**
   a. Using the Insurance Guide 1.0, develop a toolkit that will provide education and awareness for organizations regarding cyber insurance policies and best practices.

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?**
   ☐ 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. A toolkit 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?**
   ☐ 2021 ☒ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

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 Cyber Awareness and Sharing Working Group
    b. State 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. We have a sub-committee comprised of insurance brokers, corporations, and attorneys working on the content.
    b. Indiana Business Resource Council
    c. Indiana University

12. **Who should be main lead of this deliverable?**
    a. Michele Howell in conjunction with the Legal and Insurance Working Group

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?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort
    a. This will require periodic updates, at least annually.

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Continued meetings with sub-committee to finalize content. | Michele Howell | 75 | December, 2021 | |
| Review outline of toolkit for website | Legal and Insurance Working Group | 25 | Feb. 2022 | |
| Layout and test web-based toolkit | Program Communications Manger | 0 | March 2022 | |
| Finalize and launch toolkit | working group and communications manager | 0 | April 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| 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 may need to be involved |

**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 |
|---|---|---|---|---|---|---|
| Website space | Making documents available for review or download | May be within scope of current IN website maintenance | unknown | IECC state support | 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 are 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. A completed list of currently available cybersecurity coverages and services would mean success.
b. The Legal and Insurance working group collaborated with IU, ASU, IBRC, and the Indiana Attorney General to produce the first survey of Indiana businesses on Cybersecurity risk. The survey was conducted prior to the Pandemic. A follow up survey needs to be conducted to measure progress of businesses understanding of cyber risks compared to January 2020.
c. A toolkit placed on the website that allows users to quickly access specific information needed to better understand how to safeguard their business relative to cybersecurity.

**21. 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. Other states or jurisdictions are likely analyzing similar information, but we are not currently aware of concrete examples.
b. We are not aware of initiatives in other states.

**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?**

☒No ☐ Yes

a. 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.
c. Lack of budget to conduct follow up study.

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

☐No ☒ Yes

a. 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
   v. AON

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. 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)?**

☐No ☒ Yes

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

a. Indiana cybersecurity office could coordinate with the Director of Communications for Indiana University and Director of Communications for Office of Indiana Attorney General and 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 will develop a Cyber Insurance Toolkit to be provided to government and businesses by April 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

**Objective 2:** With an effective communications plan, point more than 1,000 users access the Cyber Insurance Toolkit 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

# 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?**
    ☐ 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?**
    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?**
    ☒ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

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. Cyber Awareness and Sharing Working Group; Strategic Resources Working Group, State 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. 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/Todd Vera

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?**

☐ One-time deliverable

☒ Ongoing/sustained effort

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/Todd Vera | 75 | December 2021 and annual after this review | Federal and State legislation should be monitored for changes in existing laws. |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| 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?**

| 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?**

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 are 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 cyberattacks 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. Completing a review of the cybersecurity laws and regulations and then passing the information on to key leaders 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?**

☒No ☐ Yes

a. Other states or jurisdictions are likely looking at these statistics, but we are not currently aware of concrete examples.
b. 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?**

☐No ☒ Yes

a. 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?**

☒No ☐ Yes

**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?**

☐No ☒ Yes

a. 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)?**

☐No ☒ Yes

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

a. Cybersecurity Program Director for the IECC could coordinate with Office of Indiana Attorney General communications.

## *Evaluation Methodology*

**Objective 1:** Legal and Insurance Working Group will review and distribute a list of cyber laws applicable to Indiana businesses and residents under the current landscape every year in December.

*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: Funds Transfer Fraud Fact Sheet

# Deliverable: Funds Transfer Fraud Fact Sheet

## *General Information*

1. **What is the deliverable?**
    a. Funds Transfer Fraud Fact Sheet

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?**
☐ 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. Train people on behaviors that will help save them from sending out funds for fraudulent reasons. Help explain what to look out for in terms of phishing, fraudulent requests, compromised email accounts, and other threats.

6. **What metric or measurement will be used to define success?**
    a. No observable metric. There is no way to track metrics except for anecdotal.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Any organization that participates in Electronic Funds Transfer

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

## 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. Leon Ravenna

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?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Complete Funds Transfer Worksheet | Leon Ravenna | 25 | 10/30/2021 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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. Specifically, having ways to avoid being caught by fraudulent means to send out company funds that cannot, in many cases, be recovered.

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

a. It will reduce risk be educating people as to what fraudulent funds transfers look like, how to spot and avoid these issues to avoid making fraudulent funds transfers. There are no costs except for the time to read and apply fundamental information.

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

a. Risk is primarily that people will unknowingly send out funds to fraudulent sites and then (in some cases) having to pay original vendors as well.

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

a. Only anecdotal metrics will be available. It would be possible to see if claims to the Attorney General's (A/G) office reduced year over year are, but this may be a stretch.

**21. 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

**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?**

☒No ☐ 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?**

☒No ☐ Yes

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

a. Occasional (potential bi-yearly updates)

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

a. Leon Ravenna CISO, KAR Global, Christine Collins Director, Incident Response & Investigations KAR Global and Former FBI Agent

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes,

a. Any that perform funds transfers such as Healthcare

## Communications

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

a. Chetrice Romero, Doug Swetnam

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

☐No ☒ Yes

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

a. None at this time.

## *Evaluation Methodology*

**Objective 1:** IECC Legal and Insurance Working group will develop a Funds Transfer Fraud Fact Sheet to be provided to government and businesses by January 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 Insurance – Survey Post-Covid

# Deliverable: Cyber Insurance Survey – Post-Covid

## *General Information*

1. **What is the deliverable?**
    a. In 2019 the Legal and Insurance Working Group conducted a survey with the assistance of Indiana University of Indiana businesses who have cybersecurity insurance coverage. Since 2020 and the pandemic, the landscape of cybersecurity has changed. The Legal and Insurance Working Group would like to redistribute that survey with the assistance of Indiana University of Indiana businesses who have cybersecurity insurance coverage to see what we as a state can learn from the findings.

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?**
    ☐ 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. This will require periodic updates, at least annually. 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?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. Cyber Awareness and Sharing working Group; 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?**
    a. Legal and Insurance Working Group and the Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. Lack of budget to complete new survey.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Conduct a survey of businesses for insurance coverage and cybersecurity insurance coverage. | Chair/Co-Chair with Indiana University | 0 | Qtr 1 2022 | |
| Analyze findings and report it out to the IECC and state leadership | Chair/Co-Chair with Indiana University | | | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| ¼ FTE | ¼ FTE | Survey | State of Indiana | Indiana General Assembly | Secretary of State should be involved. |

**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 |
|---|---|---|---|---|---|---|
| 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 are 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?**

☒No ☐ Yes

a. 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?**

☒No ☐ Yes

a. 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. Lack of budget to conduct survey.

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

☒No ☐ Yes

**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. Indiana University Scott Shackelford and Cybersecurity Program Director

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. 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)?**

☐No ☒ 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 with Indiana University will conduct a post-COVID survey of businesses for insurance coverage and cybersecurity insurance coverage by June 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

**Objective 2:** IECC Legal and Insurance Working Group with Indiana University will provide a report of the findings of the cyber insurance survey to the IECC by September 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

# 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 – 2019
- Business Insurance Survey and Report – 2020

# Cyber & Technology Insurance Guide - Version 1

# 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.

# Survey of Cyber Laws – 2019

# 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,<br>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:<br>(1) modifies data, a computer program, or supporting documentation;<br>(2) destroys data, a computer program, or supporting documentation; or<br>(3) discloses or takes data, a computer program, or supporting documentation that is:<br>(A) a trade secret (as defined in IC 24-2-3-2); or (B) otherwise confidential as provided by law;<br>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:<br>(1) disrupts, denies, or causes the disruption or denial of computer system services to an authorized user of the computer system services that are:<br>(A) owned by; (B) under contract to; or (C) operated for, on behalf of, or in conjunction with; another person in whole or part;<br>(2) destroys, takes, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network;<br>(3) destroys or damages a computer, computer system, or computer network; or<br>(4) introduces a computer contaminant into a computer, computer system, or computer network;<br>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:<br>(1) without the other person's consent; and<br>(2) with intent to: (A) harm or defraud another person; (B) assume another person's identity; or (C) profess to be another person;<br>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:<br>(1) with intent to harm or defraud another person;<br>(2) with intent to assume another person's identity; or<br>(3) with intent to profess to be another person;<br>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:<br>(1) identity deception (IC 35-43-5-3.5);<br>(2) synthetic identity deception (IC 35-43-5-3.8);<br>(3) fraud (IC 35-43-5-4); or<br>(4) terroristic deception (IC 35-43-5-3.6);<br>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."<br><br>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**<br>**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<br><br>12 U.S.C. §§ 1730(d), 1829b, 1951-59, et seq.<br><br>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.<br><br>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.;<br>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 -<br>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<br>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.<br><br>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<br>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.<br><br>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;<br><br>17 U.S.C. §§ 101, 104, 104A, 108, 112, 114, 117, 701, et seq.;<br><br>17 U.S.C. §§ 512, 1201–1205, 1301–1332, et seq.;<br><br>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<br><br>(Last Amended or Revised in 2002) | | Uniform Laws Annotated. Uniform Computer Information Transactions Act<br><br>(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.<br><br>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.<br><br>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.<br><br>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.<br>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<br>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;<br><br>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.<br><br>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.<br>(1) The State must comply with Federal requirements to—<br>(i) Ensure the qualifications of the providers who request Medicaid EHR incentive payments;<br>(ii) Detect improper payments; and<br>(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.<br>(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<br><br>(Amends the Government Performance and Results Act of 1993) | | Pub. L. No. 111-352<br><br>(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.<br><br>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.<br><br>The recommended practices included the following:<br>1. There must be no personal data record-keeping systems whose very existence is secret.<br>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.<br>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.<br>4. There must be a way for an individual to correct or amend a record of identifiable information about him.<br>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:<br><br>(1) collection limitation—data should be collected lawfully with the individual's consent;<br>(2) data quality—data should be relevant to a particular purpose and be accurate;<br>(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;<br>(4) use limitation—data should not be disclosed for different purposes without the consent of the individual;<br>(5) security safeguards—data should be protected by reasonable safeguards;<br>(6) openness principle—individuals should be informed about the practices and polices of those handling their personal information;<br>(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;<br>(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<br>• Notify Attorney General: Yes, if over 1000 people<br>• Notify Credit Reporting Agencies: Yes, if over 1000 people<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if: over 10,000 residents or $500,000<br>• 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<br>• Notify Attorney General: Yes, if not disclosing to residents<br>• Notify Credit Reporting Agencies: Yes, if over 1000 people<br>• If not data owner, notify data owner: Unclear<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if: over 300,000 residents or $150,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 people<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if: over 100,000 people or $50,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if: 500,000 residents or $250,000<br>• Credit Monitoring: No<br>• | 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:<br>(1) The act, use, or employment by any person of any deception, fraud, or false pretense; or<br>(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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: Yes, if over 1000 people<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if:<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 people<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if: 250,000 residents or $250,000<br>• 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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if: 500,000 residents or $250,000<br>• Credit Monitoring: Yes, 12 months<br>• 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<br>• Notify Attorney General: Yes, if over 500 residents<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay, but no more than 60 days<br>• Substitute Notice: Yes, if over 100,000 residents or $75,000<br>• Credit Monitoring: Yes, if SSN breached, 12 months<br>• 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<br>• Notify Department of Legal Affairs: Yes, if over 500<br>• Notify Credit Reporting Agencies: Yes, if over 1000 people<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if: over 500,000 residents or $250,000<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 10,000 residents<br>• If not data owner, notify data owner: Yes, within 24 hours<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if: over 100,000 residents or $50,000<br>• 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<br>• Notify Attorney General: Yes, if over 1000 residents<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 200,000 residents or $100,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 50,000 residents or $25,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 500,000 residents or $250,000<br>• 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<br>• Notify Attorney General: Yes, if over 500 residents<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 350,000 residents or $250,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 5,000 residents or $100,000<br>• 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:<br>(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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 people<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if: 500,000 residents or $250,000<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 50,000 residents or $250,000<br>• Credit Monitoring: No<br>• 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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 1,000 people or $5,000<br>• 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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: Yes, over 1000<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay and several day requirements<br>• Substitute Notice: Yes, if over 175,000 residents or $100,000<br>• Credit Monitoring: No<br>• Other: | $1,000 per violation: Md. Code, Com. Law §§ 14-3508, 13-410 | Division of Consumer Protection: Md. Code Comm<br>. 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<br>. Law §§ 13-403 and 13-410 |
| **Unfair, Deceptive, or Abusive Acts and Practices** | Md. Code Comm<br>. 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<br>. Law §§ 13-403 and 13-410 |
| | | | | |
| **Massachusetts Breach Notification Law** | Mass. Gen. Laws Ch. 93H § 1 | • Notify Affected Residents: Yes<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: Attorney General<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 500,00 residents or $250,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 500,000 residents or $250,000<br>• 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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: Yes, if over 500 residents. Notification in 48 hours.<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 500,000 residents or $250,000<br>• 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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 5,000 residents or $5,000<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: Yes, if over 1000 residents<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 150,000 residents or $150,000<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: Yes, coordination provision<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 500,000 residents or $250,000<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 100,000 residents or $75,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 500,000 residents or $250,000<br>• 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<br>• Notify Attorney General: Yes, if subject to N.H. Rev. Stat. § 358-A:3(I)<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: As soon as possible<br>• Substitute Notice: Yes, if over 1,000 residents or $5,000<br>• 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<br>• Notify Attorney General: Yes, prior to notification to customers<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 500,000 residents or $250,000<br>• Credit Monitoring: No<br>• 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<br>• Notify Attorney General: Yes, if over 1000 residents<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: No later than 45 days after the breach discovery date<br>• Substitute Notice: Yes, if over 50,000 residents or $100,000<br>• 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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: Yes, if over 5000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 500,000 residents or $250,000<br>• 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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 500,000 or $250,000<br>• Credit Monitoring: No<br>• 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<br>• Notify Attorney General: Yes, if over 250 people<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 500,000 or $250,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: No longer than 45 days following the breach discovery date<br>• Substitute Notice: Yes, if over 500,000 residents or $250,000<br>• Credit Monitoring: No<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 100,000 residents or $50,000<br>• 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<br>• Notify Attorney General: Yes, if over 250 residents<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 350,000 residents and $250,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 175,000 people or $100,000<br>• 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<br>• Notify Attorney General: Yes<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: Yes, if over 1000 residents<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: Yes, if over 250 residents<br>• Notify Credit Reporting Agencies: Yes<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Within 60 days of breach discovery date.<br>• Substitute Notice: Yes, if over 500,000 people or $250,000<br>• Credit Monitoring:<br>• 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:<br>(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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes, within 45 of breach discovery date<br>• How many days to Notify: Within 45 of breach discovery date<br>• Substitute Notice: Yes, if over 500,000 people or $250,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 10,000 people<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if: 500,000 people or $250,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Not allowed<br>• 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:<br>(a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and<br>(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<br>• Notify Attorney General: Yes, within 14 business days of breach discovery<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 5,000 residents or $5,000<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: Yes, if over 1000 residents<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 100,000 residents or $50,000<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: Yes, if over 500 residents<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: No more than 45 days after the breach discovery<br>• Substitute Notice: Yes, if over 500,000 residents or $250,000<br>• Credit Monitoring:<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 100,000 residents or $50,000<br>• Credit Monitoring: No<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Within 45 days of the breach discovery date<br>• Substitute Notice: Yes, see statute<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, see statute<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: Yes, if over 1000 residents<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 100,000 or $50,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 5,000 residents or $10,000<br>• Credit Monitoring: No<br>• 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<br>• Notify the Secretary of Consumer Affairs: Yes, within 10 days<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 100,000 people or $100,000<br>• 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<br>• Notify Attorney General: No<br>• Notify Credit Reporting Agencies: No<br>• If not data owner, notify data owner: Yes<br>• How many days to Notify: Without unreasonable delay<br>• Substitute Notice: Yes, if over 50,000 residents or $100,000<br>• Credit Monitoring: No<br>• 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<br><br>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.<br><br>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:<br>CSA Security, Trust & Assurance Registry (STAR)<br>Certificate of Cloud Security Knowledge (CCSK)<br>Certified Cloud Security Professional (CCSP)<br>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)<br>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.<br><br>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.<br><br>Guidance includes:<br><br>Online Banking: https://www.ffiec.gov/pdf/authentication_guidance.pdf<br>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/ |

# Business Insurance Survey and Report – 2020

# State of Hoosier Cybersecurity

2020

December 2020

Prepared for

Indiana Executive Council on Cybersecurity

By

Kelley School of Business, Indiana University
Indiana Business Research Center
Anne Boustead JD, PhD (University of Arizona), Scott Shackelford JD, PhD (Indiana University)

Special thanks to Jay Bhatia and Eric Spencer for their invaluable research support in this project. We would also like to thank the anonymous respondents who participated in our survey on behalf of their organizations, and to Stephen Vina, and Professors Asaf Lubin and Angie Raymond for their helpful comments and suggestions.




# Table of Contents

## Index of Figures



## Contact Information

For more information about this report, contact the Indiana Business Research Center at (812) 855-5507 or email ibrc@iupui.edu. Professor Shackelford may be reached at sjshacke@indiana.edu.

# Executive Summary

As is the case in many jurisdictions, public and private organizations in Indiana are unfortunately no stranger to cyber attacks. Counties across the state such as Lake,[1] Lawrence,[2] and LaPorte[3] have been targeted by criminals in recent ransomware campaigns, leading to hundreds of thousands in losses. Healthcare providers such as Hancock Memorial Hospital have been similarly breached, as have universities, small business, utilities, and school corporations.[4] Yet it has proven difficult to understand the full scope of these cyber threats, and how Hoosier organizations are attempting to prevent and respond to them.

To get a more complete picture of Hoosier cyber risk planning, the Legal and Insurance working group of the Indiana Executive Cybersecurity Council, in collaboration with researchers at Indiana University and the University of Arizona, conducted this study to help explore how Indiana organizations perceive and manage cyber risks. We pay particular attention to the role of insurance as part of an overarching cyber risk mitigation strategy.

The report is broken down into the following sections. Section 1 offers background on the technical, organizational, and legal dimensions of the cyber threat, along with a policy review highlighting recent primarily state-level efforts in Indiana and beyond to better manage cyber risk. Section 2 reviews the methods used in this study. Section 3 summarizes our results, paying particular attention to such topics as risk perceptions, management, and the evolving role of cyber risk insurance. Section 4 concludes the study with a look at policy opportunities to address the vulnerabilities and governance gaps revealed by the survey.

This goal of this report is to provide business leaders, policymakers, law enforcement professionals, and all Hoosiers with important information about cyber readiness, help organizations of all sizes better understand current cyber threats facing Indiana, and describe current efforts to address them. In the end, cybersecurity is a team sport, and we're all in this together.

---

[1] *See* Anna Ortiz, *Lake County, Ind., Sheriff's Email Online After Cyberattack*, GOVTECH (Sept. 9, 2019), https://www.govtech.com/security/Lake-County-Ind-Sheriffs-Email-Online-After-Cyberattack.html.

[2] *See* Rich Van Wyk, *Cyberattack Knocks out Lawrence County Government Computers*, WTHR (Feb. 13, 2020), https://www.wthr.com/article/news/local/indiana/cyberattack-knocks-out-lawrence-county-government-computers/531-637645fa-2797-416f-b890-e95112333106.

[3] *See* Mike Lowe, *Laporte County Government Pays $130K Ransom to Hackers*, WGNTV (July 18, 2019), https://wgntv.com/news/laporte-county-government-pays-130k-ransom-to-hackers/.

[4] *See* Patrick Howell O'Neill, *Indiana Hospital Shuts Down Systems After Ransomware Attack*, CYBERSCOOP (Jan. 15, 2018), https://www.cyberscoop.com/hancock-hospital-ransomware/.

# Key Findings

- The Indiana organizations who responded to this survey generally expressed concern about the risk of a cyber incident. Less than 5% of respondents indicated that they were not at all concerned about the risk of a cyber incident, while over 46% of respondents identified as somewhat concerned and almost 49% identified as very concerned. When asked about the specific types of cyber incidents they were concerned about, respondents most frequently indicated concern about malware attacks (86% of respondents), phishing attacks (76% of respondents), and ransomware attacks (74% of respondents).
- In order to understand Indiana organizations' previous experiences with and responses to cyber incidents, respondents were asked whether their organization had experienced a successful cyber incident in the past three years. Approximately 19% of respondents indicated that they had experienced a successful cyber incident during this timeframe, while 67% of respondents indicated that their organization did not experience a successful cyber incident and 13% were either not sure or declined to provide an answer. Of respondents who indicated that their organization had experienced a successful cyber incident in the past three years, 50% indicated that none of these incidents resulted in data loss and 31% indicated that less than five of these incidents resulted in data loss.
- The vast majority – over 82% – of respondents indicated that their organization had taken steps to prevent a cyber incident; about 7% indicated that their organization had *not* taken steps to prevent cyber incidents, and about 9% indicated that they were not sure. Of respondents who indicated that they had taken steps to prevent cyber incidents, 95% had installed antivirus software, while over 75% had updated/patched software, and over 70% had provided their employees with training to reduce cyber-related risks. Seventeen respondents indicated that they had used mechanisms to prevent cyber incidents other than the options provided by the survey; these respondents described a broad range of alternative mechanisms including installing firewalls and spam filters, adopting multi-factor authentication, and hiring a cybersecurity firm to advise on defenses.
- Respondents who indicated that their organization had not taken steps to prevent cyber incidents were then asked why these steps had not been taken. Of those respondents who indicated that their organization had not taken steps to adopt cyber incident prevention mechanisms, slightly more than half attributed this decision to the organization being unsure what to do, while 40% explained that their organization did not think it was at risk. Perhaps most interestingly, no respondents indicated that their organization did not adopt cyber incident prevention mechanisms because they believed those mechanisms to be ineffective.
- In order to understand how Indiana organizations are protecting their systems and information, respondents were then asked whether their organization had adopted certain cybersecurity practices. Of the 178 respondents who answered the question, slightly less than half indicated that their organization had adopted automatic updating of operation systems and software and implementation of remote backups.
- The development and documentation of incident planning and response is a key cybersecurity practice. About 27% of respondents reported that their organization had written cyber incident planning and response documentation, with more than half indicating that their organization did not have such documentation and the remainder of respondents being uncertain or unresponsive.

- Cybersecurity response is also shaped by the people selected to lead this response. When asked who at their organization was ultimately responsible for managing cyber risk, about 15% of respondents indicated this role was filled by their Chief Information Officer, and about 14% indicated that this role was filled by their Chief Executive Officer. Interestingly, almost half of respondents elected to write in their own response to this question, with a common response being that this role was fulfilled by an information technology manager, director, or department (and several respondents indicating that no one served in this role).
- Organizations concerned about their cybersecurity have a range of external tools and frameworks available to help guide their decision making in this area. Fifty-eight respondents stated that their organization consulted an externally developed tool, framework, or control when making decisions about cyber practices. Among respondents who indicated that their organization used an externally developed framework to guide their cybersecurity decision making, the most commonly used framework was the NIST Cybersecurity Framework, which had been adopted by 58% of those organizations adopting a framework and 36% had adopted the Center for Internet Security (CIS) Critical Security Controls.
- About half of respondents indicated that their organization had cyber risk insurance; 26% indicated that their organization did not have cyber risk insurance; remaining respondents were either unsure or declined to answer. Respondents were next asked why their organization obtained a cyber risk insurance policy. Half of respondents described the decision to obtain cyber risk insurance as a response to news reports on cyber incidents. A large minority (40.82%) of respondents provided another reason for obtaining cyber risk insurance. These reasons included insurance agent recommendations or inclusion of cyber coverage in a general policy, response to cybersecurity trainings by trade organizations or other outside groups, and a perception that obtaining this insurance "just made business sense."

# Understanding Cyber Risk

Although many consumers and businesses think of cyber risk in terms of hacked computers and stolen credit card numbers, there is a rapidly expanding universe of vulnerabilities fed in part by the explosion in Internet-connected devices and services comprising the Internet of Things. Even before the COVID-19 pandemic, which shifted many personal and professional activities online, cyber criminals, terrorists, hacktivists, and even foreign nation states were exploiting these vulnerabilities to steal identities, intellectual property, and compromise critical infrastructure. In this section, we begin by outlining the technical, economic, and legal dimensions of the cyber threat landscape currently facing organizations. We then turn to recommendations commonly made to organizations seeking to manage their cyber risk profiles, summarizing these best practices in terms of three steps: being aware, being organized, and being proactive. Finally, we discuss several issues that are currently changing the cyber risk landscape.

## A. Cyber Threat Dimensions

Organizations currently face cyber risks across multiple dimensions: the myriad technical threats to information and systems pose serious economic threats across many sectors. Furthermore, the complex, patchwork legal landscape governing cybersecurity and privacy in the United States poses a challenge to businesses seeking to understand the protections that apply to them and the regulations they must comply with.

### 1. Technical

Technical vulnerabilities pervade modern business, and society. Smart phones can be compromised to be used as microphones even when they appear to be turned off.[5] Internet-connected lights and kitchen appliances can be hijacked to launch cyber attacks.[6] Internet traffic can be rerouted to servers around the world without the user's awareness.[7] Supply chain vulnerabilities and weak encryption can lead to a cascade of failures, yet are hard to identify and address.[8] Each of these cyber risks, as with so many others, require a suite of corporate

[5] *See* Darlene Storm, *New Attacks Secretly Use Smartphone Cameras, Speakers, and Microphones*, COMPUTER WORLD (Aug. 20, 2014), https://www.computerworld.com/article/2598704/new-attacks-secretly-use-smartphone-cameras--speakers-and-microphones.html.

[6] *See* Sarah Murray, *When Fridges Attack*: Why Hackers Could Target the Grid, FIN. TIMES (Oct. 17, 2018), https://www.ft.com/content/2c17ff5e-4f02-11e8-ac41-759eee1efb74.

[7] *See* Zak Doffmann, *Russia and China 'Hijack' Your Internet Traffic: Here's What You Do*, FORBES (Apr. 18, 2020), https://www.forbes.com/sites/zakdoffman/2020/04/18/russia-and-china-behind-internet-hijack-risk-heres-how-to-check-youre-now-secure/#2b936c395b16.

[8] *See* Nate Berg, *Starbudks, PepsiCo, and BMW Partner to Fix a Global Problem Worth Trillions*, FAST COMPANY (Aug. 6, 2020), https://www.fastcompany.com/90536448/starbucks-pepsico-and-bmw-partner-to-fix-a-global-problem-worth-trillions; Caroline Dowling, *How Vulnerable is Your Supply Chain?*, INDUSTRY WK. (Dec. 6, 2012),

governance and policy responses. The problem is vexing given both the complexity and scale of the issue, with reports of novel cyber attacks being launched every thirty-nine seconds.[9]

## 2. Economic

Successful cyber attacks can cause serious and long-lasting impacts on organizations, including but not limited to financial damages, compromised personally identifiable information, breaches of critical infrastructure, tarnished reputations, and a loss of consumer confidence.[10] Managing the fallout from a data breach can be a challenging and costly endeavor. While this pertains to most organizations, it is especially true for small and midsize businesses (SMBs). Cybercrime has become a significant cost center for these firms, with a 2019 survey revealing that 58% of executives thought that data breaches were a more significant concern than incidents like fires, floods, and physical break-ins combined.[11] This is both true of midmarket firms, as well as larger organizations; indeed, perhaps counterintuitively the bigger the company, the less it spends per employee for cybersecurity owing to economies of scale combined with a lack of focus on cybersecurity issues.[12] For example, a 2019 cybersecurity IBM survey of large firms found that only 16% of respondents considered user security awareness training to be a priority.[13]

In addition to businesses, attacks on local governments are more salient than ever. Governments often misperceive the potential complexity of a cyber attack, which can cause sensitive data like bank information, government processes, municipal employee records to become vulnerable. Just like businesses, local governments have to work within the lack of financial resources to tackle cybersecurity challenges, with average state or local government agencies spending less than 5% of their IT budget on cybersecurity.[14]

Despite these risks, and with a few notable exceptions such as the financial industry where cybersecurity spending is high due to the alignment of incentives through the imposition of

---

https://www.industryweek.com/supply-chain/customer-relationships/article/21959294/how-vulnerable-is-your-supply-chain.

[9] *See Hackers Attack Every 39 Seconds*, SEC. MAG. (Feb. 10, 2017), https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds.

[10] *See Press Release: New Study Reveals Impact of Cyberattacks on Consumer Confidence, Corporate Reputation*, DHM RES. (Oct. 3, 2019), https://www.dhmresearch.com/press-release-new-study-reveals-impact-of-cyberattacks-on-consumer-confidence-corporate-reputation/.

[11] Survey: *Cybercrime More Devastating to SMBs than Other Threats Combined*, GLOBE NEWS WIRE (Feb. 26, 2019), https://www.globenewswire.com/news-release/2019/02/26/1742542/0/en/Survey-Cybercrime-More-Devastating-to-SMBs-than-Other-Threats-Combined.html.

[12] *White Hat, Black Hat and the Emergence of the Gray Hat: The True Costs of Cybercrime* (Osterman Res. White Paper, Aug. 8, 2018), http://resources.malwarebytes.com/files/2018/08/GLOBAL-White-Hat-Black-Hat-and-the-Emergence-of-the-Gray-Hat-The-True-Costs-of-Cybercrime_Sponsored-by-Malwarebytes.pdf.

[13] *IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them*, IBM (Apr. 11, 2019), https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them.

[14] *See Congress Moving Closer Toward Cybersecurity Aid to State and Local Governments*, ST. SCOOP (Sept. 23, 2019), https://statescoop.com/congress-moving-closer-toward-cybersecurity-aid-to-state-and-local-governments/.

liability for breaches, the overall growth in cybersecurity spending remains relatively low according to Gartner Research. Spending on cybersecurity grew at 12% compound annual growth rate (CAGR) in 2018, and it is projected to decline to 7% CAGR by 2023.[15] Part of this decline may be explained by more boards pushing back and asking for improved data and understanding of what increased cybersecurity spending has achieved after years of heavy investment.[16] And, to date, many organizations have not faced significant fines, litigation costs, or incentives to change behavior. A 2018 report from Schinichi Kamiya and colleagues found that "[a]fter suffering a breach of customers' personal data, the average attacked firm loses 1.1 percent of its market value and experiences a 3.2 percentage point drop in its year-on-year sales growth rate."[17] In fact, some firms, such as LinkedIn, saw their stock prices actually rise following significant cyber attacks.[18] As a result, an open debate is underway about whether or not we are experiencing a market failure in cybersecurity and, if so, what role state and federal governments should have in addressing it.

## 3. Legal

Unlike other jurisdictions such as the European Union, the U.S. government has no comprehensive federal law that regulates information security, cybersecurity, and privacy throughout the country. As a result, many states have passed laws to address these governance gaps. This creates a unique challenge for organizations that conduct business across state lines, as these areas are currently regulated by a piecemeal of sector-specific federal laws and state legislation.

Some states have been more active in adopting cybersecurity laws than others, although some categories of cybersecurity have been commonly adopted. Figure 1 below shows variation in the number of cybersecurity laws adopted by states, taking into account laws that expressly criminalize phishing, distributed denial-of-service (DDoS) attacks, spyware, and ransomware, as well as the creation of a state-wide cybersecurity task force and adoption of the NAIC data security model law for the cyber-insurance industry. Furthermore, even states that have adopted similar laws may have implemented them at different times. For example, Figure 2 summarizes the year each state passed their Breach Notification Law.

Legislative policymaking is ongoing in this area. Thirty-eight states, Washington, D.C., and Puerto Rico have considered nearly 300 bills or resolutions that deal significantly with cybersecurity in 2020,[19] and 31 states enacted new cybersecurity legislation so far this year.

---

[15] *Id*.

[16] *See* Louis Columbus*, Why Cybersecurity is Really a Business Problem*, FORBES (June 25, 2020), https://www.forbes.com/sites/louiscolumbus/2020/06/25/why-cybersecurity-is-really-a-business-problem/#362b6134436c.

[17] Shinichi Kamiya, *What is the Impact of Successful Cyberattacks on Target Firms?*, NAT'L BUREAU OF ECON. RES. (NBER Working Paper No. 24409, 2018), http://www.nber.org/papers/w24409.

[18] *See* Nicole Perlroth, *Lax Security at LinkedIn Is Laid Bare*, N.Y. TIMES, June 10, 2012, at B1.

[19] Cybersecurity Legislation 2020, https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx (last visited Aug. 11, 2020).

This marks a significant rise from 2015 when only 26 states considered resolutions and just eight states enacting legislation. Some of the areas seeing the most recent legislative activity include:

- Increasing penalties for cybercrimes.
- Regulating cybersecurity within the insurance industry.
- Regulating government agencies to implement training and security policies and practices to better improve incidence response and preparedness.
- Creating task forces and commissions to study or advise on cybersecurity issues.
- Supporting programs and incentives for cybersecurity training and education.

OBJ

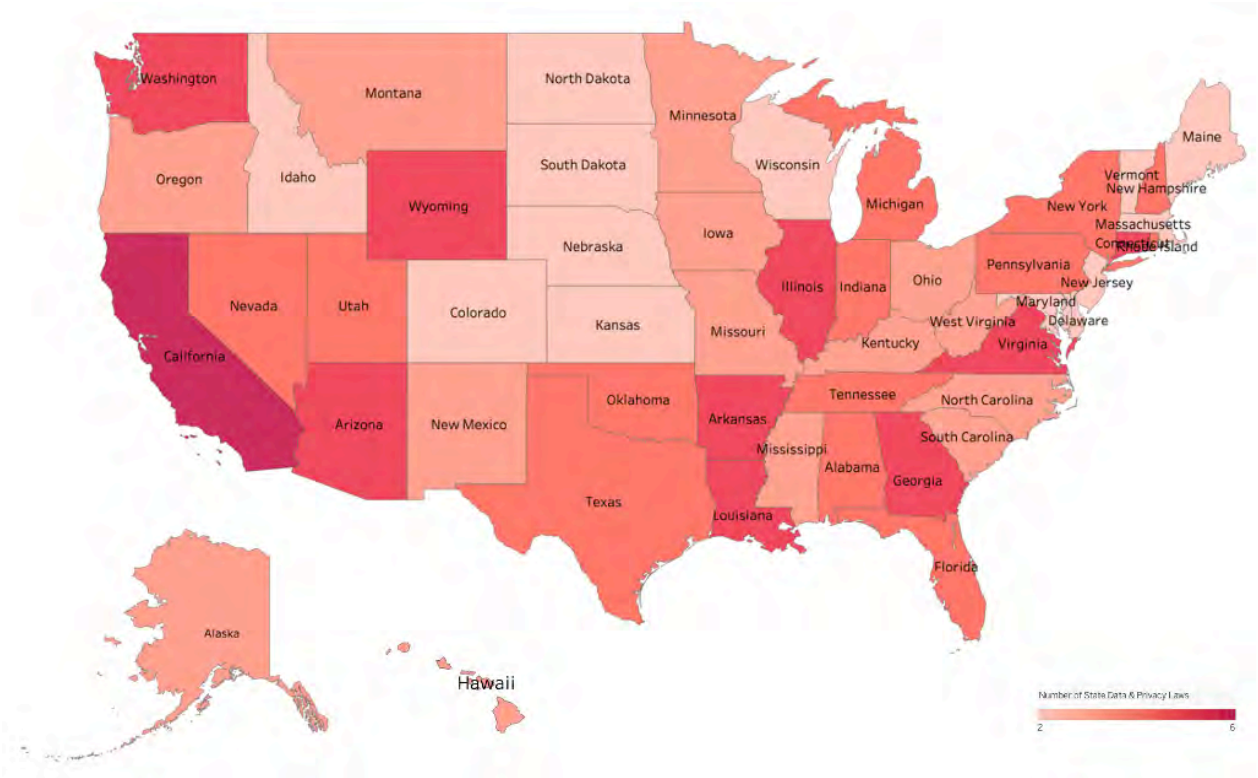



**Figure 1: State-Level Cybersecurity Laws (2020)**

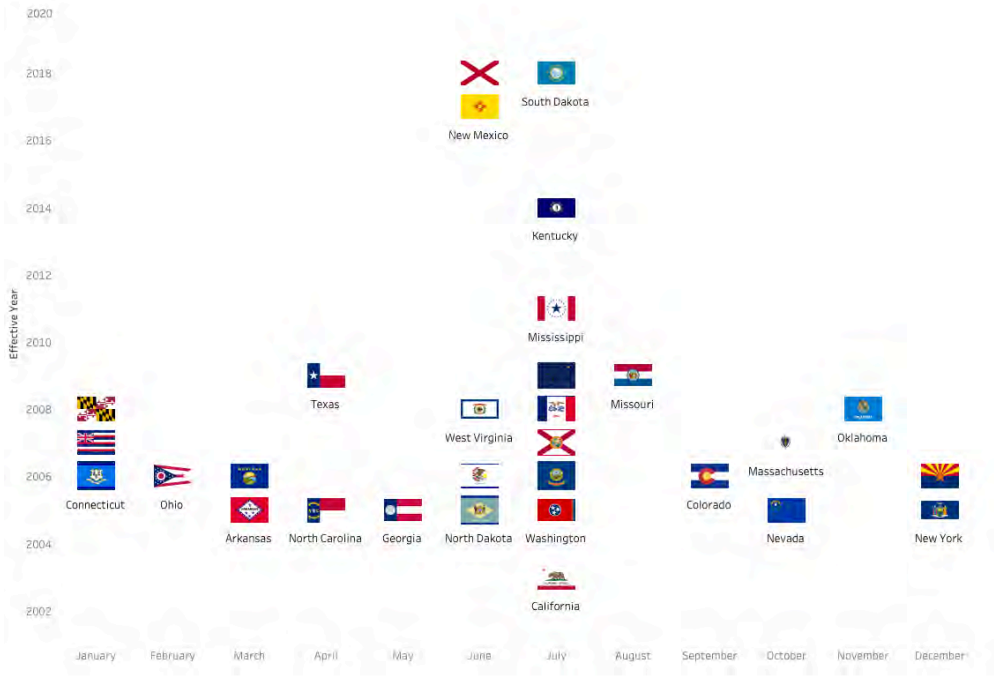



**Figure 2: State Breach Notification Laws**

# B. Steps to Managing Cyber Risks

Analysts have recommended that organizations of all sizes manage cyber risk by (1) being aware, (2) being organized, and (3) being proactive.[20] As we discuss below, each of these steps can potentially include a wide range of technical and business activities.

## 1. Be Aware

Managers and policymakers need to keep up to date on the growing variety of cyber threats facing their organizations, especially as an increasing number of workers are working remotely. Phishing and ransomware campaigns are especially prevalent during the pandemic.[21] Cybercriminals have taken advantage of the current global health crisis, for example, and the new technical configurations that result from a remote workforce to multiply the number of attacks.[22] In response, organizations of all sizes need to be aware of the variety of cyber threats facing their organizations. A range of cybersecurity best practices can help firms better

[20] Scott J. Shackelford, *The Three 'B's' of Cybersecurity for Small Businesses*, CONVERSATION (Apr. 17, 2017), https://theconversation.com/the-three-bs-of-cybersecurity-for-small-businesses-76259.

[21] *See Understanding and Dealing with Phishing During the Covid-19 Pandemic*, ENISA (May 6, 2020), https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic.

[22] *See* Steve Grobman, *Adjusting to the New Security Realities of a Remote Workforce*, CYBER SCOOP (May 27, 2020), https://www.cyberscoop.com/steve-grobman-new-cybersecurity-realities-remote-workforce/.

understand their vulnerabilities, including network traffic analysis using deep packet inspection.[23]

## 2. Be Organized

Protecting an organizations' physical infrastructure is only the first step in safeguarding its assets; in many ways, digital assets and information is increasingly the lifeblood of both government entities and private firms. One example of this fact is the extent to which the intangible assets comprising the S&P 500 flipped from the 1970s to 2018, at which point intangibles such as intellectual property and reputation comprised 84% of corporate value.[24] Organization is vital to protect such invaluable digital assets, yet even a computer that is "air gapped," or unplugged from the public Internet may still be accessible via flash drive or rewritable CD introduced by an insider threat. Large companies like Sony did not even have a Chief Information Security Officer until relatively recently. It hired one in the aftermath of its 2011 breach, but that did not save them from being breached again in 2014.[25] As is explored below in the Results section, still in 2020 both leadership structures and accountability remains muddy in too many organizations across Indiana.

## 3. Be Proactive

In general, the best cyber defense is a healthy skepticism and proactive vigilance backed up by a robust program of cyber hygiene and an updated incident response plan. Employees who do not have appropriate cybersecurity skills can unintentionally create vulnerabilities in a network. For example, it has been reported that 91% of cyber-attacks start with a phishing email – an issue that may be addressable by training.[26] Network security policies ensure that employees have access to the correct and appropriate information, and play a key role in preventing breaches from occurring. However, designing security policies to strike the correct balance between security and convenience is not an easy undertaking. For example, consider the difficulty of monitoring employees who are working remotely. One study found that 78% of IT specialists reported that their end users had set up unapproved services and applications, which increased

---

[23] *See* Duncan Geere, *How Deep Packet Inspection Works*, WIRED (Apr. 27, 2012), https://www.wired.co.uk/article/how-deep-packet-inspection-works. SaaS-based web gateway architecture has also been a proposed solution that can provide essential security controls to safeguard users visiting websites. In addition to protecting businesses from incoming threats and outgoing information exfiltration, it also allows organizations to apply similar corporate internet access policies to the increasing number of remote workers due to the COVID-19 pandemic.

[24] *See* Bruce Berman, *$21 Trillion in U.S. Intangible Assets is 84% of S&P 500 Value*, IP CLOSE UP (June 4, 2019), https://ipcloseup.com/2019/06/04/21-trillion-in-u-s-intangible-asset-value-is-84-of-sp-500-value-ip-rights-and-reputation-included/.

[25] *See* John Gaudiosi, *Why Sony Didn't Learn From its 2011 Hack*, FORTUNE (Dec. 24, 2014), https://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

[26] *91% of Cyber Attacks Start with a Phishing Email: Here's How to Protect Against Phishing*, DIGITAL GUARDIAN (July 26, 2017), https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing.

the chance of a potential unmanaged risk.[27] Hiring qualified cybersecurity personnel is another source of concern, as demonstrated by the fact that there are currently more than 3.5 million unfilled cybersecurity jobs.[28] In general, it is essential that organizations have resources and tools in place that allow them to adhere to and manage security policies. Anything that forces people to drastically change the way they work or results in an organization's lack of agility is counterproductive. An ideal solution should offer increased security entwined with business agility, which is an arena where cyber risk insurance can help.

# C. Current Trends in Addressing Cyber Risk

Cyber risk evolves as quickly as the technology, social context, and policies underlying information systems. Although this evolution occurs in myriad ways, in this section we focus on three of the most prominent issues in cyber risk management today: the continuing importance of cyber risk insurance, the emergence of Artificial Intelligence (AI) as a tool for identifying and responding to cyber incidents, and the impact of the COVID-19 pandemic on technology practices and risks.

## 1. Cyber Risk Insurance

Cyber risk insurance has long been thought of as an integral component to managing cyber risk. Insurance firms have been experimenting with cyber risk insurance policies for decades.[29] By some estimates the market is worth more than $2.5 billion in 2020, with projections that it could triple by 2030,[30] a trend that could be reinforced by regulatory developments such as the California Consumer Privacy Act (CCPA) or the EU's General Data Protection Regulation (GDPR).[31] Indeed, U.S. companies are increasingly eyeing cyber insurance as they potentially face millions of dollars in liability under CCPA, under which state residents can seek up to $750

[27] *See The 2020 State of IT*, Spiceworks, https://www.spiceworks.com/marketing/state-of-it/report/ (last visited Aug. 10, 2020).

[28] *See The Dearth of Skilled. Cybersecurity Personnel*, SC MAG. (Jan. 23, 2020), https://www.scmagazine.com/home/advertise/the-dearth-of-skilled-cybersecurity-personnel/. In the absence of trained personnel, network security operations can turn to policy-based automation to reduce incomprehensibility, improve visibility, and focus resources on more complex tasks to improve operational efficiencies that directly impact the upshot of the business.

[29] Jon Swartz, *Firms' Hacking-Related Insurance Costs Soar*, USA TODAY (Feb. 9, 2003), http://usatoday30.usatoday.com/tech/news/computersecurity/2003-02-09-hacker_x.htm.

[30] *Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience*, PWC (2020), https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html.

[31] *See* Carolyn Cohn, *Europe's New Data Privacy Law Boosts Cyber Insurance Sales*, INSURANCE J. (May 22, 2018), https://www.insurancejournal.com/news/international/2018/05/22/489977.htm ("Insurers say the directive, together with major cyber attacks like last year's WannaCry and NotPetya viruses, is driving demand in Europe for cyber insurance – a sector seen as relatively profitable.").

per data security incident. The CCPA also directs the California Attorney General to take enforcement actions for privacy violations.[32]

In addition to protecting organizations against financial fallout from cyber incidents, organizations can use cyber risk insurance to inform their security practices in other ways. For example, insurers can use tactics like cyber-meteorology to audit companies against cyber risks and help them prioritize their security efforts.[33] The insurance industry has also focused extensively on their own cybersecurity practices. Model laws like the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law seek to establish data security standards for regulators and insurers in order to mitigate the potential damage of future data breaches. This Model Law, which has been enacted in at least 11 states as of September 2020, requires insurers and other entities licensed by a state department of insurance to develop, implement, and maintain an information security program based on a recognized risk assessment tool, with a designated employee in charge of the information security program. The model does not create a private cause of action, nor does it limit an already-existing private right of action. As such, it is less a new approach to regulating cyber risk insurance than an encouragement for covered insurance providers to adopt an approved set of cybersecurity tools and frameworks.

However, with 49 states still not mandating cyber insurance, adoption has been slow. Deloitte's 2019 Middle Market Cyber Insurance Survey reported cost and coverage limits being the main deterrent from purchasing cyber risk insurance.[34] However, much is still unknown about how companies decide whether to adopt cyber risk insurance, and the broader role that cyber risk insurance plays in cyber risk mitigation practices, which is a key topic on which this survey focuses.

Moreover, cyber risk insurance does not protect companies against all types of cyber risks. The full impact of some potential risks may be difficult to quantify and thus difficult to fully insure. Insurance policies may exclude coverage of incidents that happen under certain circumstances, such as a cyber-attack that is attributed back to a foreign nation that may be defined as an act of war. Businesses must carefully review policies to ensure that their expectations about what types of incidents are covered aligns with their policies, which can create barriers to adopting policies.

## 2. Artificial Intelligence

Artificial intelligence (AI) has been sought as the next frontier for protection against cyber threats with some organizations predicting AI-powered technologies to triple by 2021.[35] An

---

[32] *See* Daniel R. Stoller, *Cyber Insurance Purchases Will Surge With California Privacy Law*, BLOOMBERG L. (Feb. 5, 2020), https://news.bloomberglaw.com/privacy-and-data-security/cyber-insurance-purchases-will-surge-with-california-privacy-law.

[33] *See* Vishaal Hariprasad, *Introducing 'Cyber Meteorology:' A New Strategy for Cyber Insurance*, DARK READING (Feb. 3, 2020), https://www.darkreading.com/risk/introducing-cyber-meteorology-a-new-strategy-for-cyber-insurance-/d/d-id/1336924.

[34] Julie Bernard, *Overcoming Challenges to Cyber Insurance Growth*, DELOITTE (Mar. 16, 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html.

[35] *The 2020 State of IT*, *supra* note 27.

automated, zero-time prevention platform can reduce the array of duties typically carried out by a cybersecurity team, which helps mitigate the prevailing cybersecurity workforce shortage, though no piece of software however advanced can replace a well-trained and well-rounded cybersecurity professional. Automated systems can, though, create alerts about anomalous activities that need to be investigated by human analysts, which can turn out to be benign. Moreover, as new threats arise, security solutions that use artificial intelligence must be re-trained to keep up.[36] Deep learning prediction models can produce a far lower level of false positives than traditional AI systems, which typically experience an approximately 1% false positive rate.[37] It is designed to automatically identify the relevant features of a malicious file or vector without engineering from a cybersecurity expert.

## 3. Cybersecurity During the Pandemic

CIOs and CISOs have been under intense pressure to meet the needs of homebound workers, while concurrently needing to take added steps to safeguard their enterprise networks. Organizations recognize the new risks associated with new types of employees working from home that have not done so prior to the pandemic. Mitigating the risks of a remote workforce largely comes down to ensuring the business is using the right security and that IT leaders are educating their employees on best practices around security as we navigate this crisis.

From an organizational standpoint, it is now more critical than ever to have the right technology in place and to make sure equipment is up to date and secure. It is also crucial for remote employees to exercise good cyber-hygiene. Organizations attempting to decide how to change their cybersecurity practices in light of COVID-19-related changed to work practices may find it helpful to consult decision-making frameworks such as the NIST Cybersecurity Framework or the Indiana University Center for Applied Cybersecurity Research Information Security Practice Principles.

COVID-19 may also change the planned use of cyber risk insurance, potentially for many years to come. The Cowbell Economic Impact of Cyber Insurance reported 65% of small and mid-Size Enterprises in the U.S plan to spend more on cybersecurity insurance over the next two years. More than half believe the cost of insurance is well worth the protection, on average, firms opt for cybersecurity insurance coverage limits of about 0.14% of revenue. By comparison, only 58% of large US-based enterprises plan to spend more on cyber-insurance over the next two years.[38]

---

[36] *Id*.

[37] *See* Abhimanyu S. Ahuja, *The Impact of Artificial Intelligence in Medicine on the Future Role of the Physician*, PEERJ (2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6779111/.

[38] *See Survey Results: The Economic Impact of Cyber Insurance*, COWBELL (June 2020), https://cowbell.insure/wp-content/uploads/2020/06/Cowbell-Cyber-data-report.pdf.

# Methods

## A. Aims of this Study

Given the multifaceted cyber threat landscape and the universality of cyber risk concerns to organizations today, it is to be expected that organizations will adopt different approaches to protecting their information and computer systems. These approaches will frequently be difficult to observe without querying organizations directly, as the steps an organization takes to buttress their cybersecurity postures may not be obvious from the outside. However, policymakers, analysts, and organizations themselves can benefit from a clearer description of this decision-making process. Better identification of the factors that organizations consider when making cybersecurity decisions can help policymakers develop incentives to promote decisions that protect consumers – and identify barriers to good decision-making. Analysts can conduct evaluations of cybersecurity policies in order to help identify which policies can be supported by empirical evidence. Organizations may benefit by better understanding the cybersecurity decision-making of their peers, as this may help them identify the standards of their industry.

In order to contribute to our current understanding of cybersecurity decision-making, we conducted a survey of Indiana organizations to query them about their perceptions of cyber risk, how their organization manages these risks, and the role of cyber risk insurance in this decision-making process. The content and distribution of this survey are described in the remainder of this section; the next section presents a summary of key results.

## B. Survey Development and Distribution

We began this study by consulting with a variety of stakeholders on both the general topics that should be addressed by a cyber risk survey, and any specific questions that they would think it necessary to include. We focused in particular on questions that would elicit information that would be most likely to be useful to cybersecurity decision-makers on both the governmental and organizational levels. Through this process, we identified several key topics to focus on, namely cyber risk perceptions, cyber risk management and planning, and cyber risk insurance use/non-use. We drafted questions to address each of these decision-making dimensions. These questions were then vetted for both completeness and clarity by cybersecurity analysts and stakeholders in order to maximize the likelihood that we would obtain useful information and ensure that would be understandable to potential respondents. The finished survey protocol is provided in Appendix B.

This survey was distributed in partnership with the Indiana Executive Cybersecurity Council and the Indiana Business Research Center. A solicitation and link to the survey was sent to an extensive mailing list of more than 3,000 public and private organizations in Indiana. We received 336 responses, including 197 complete responses and 139 incomplete responses. Incomplete responses were dropped for analysis. This left us with an overall response rate of 6%.

Figure 3 below describes the number of employees and geographic scope of respondent organizations. As can be seen, respondents represented a range of organizational sizes, but most commonly reported that their organization employed 1-10 people. Similarly, respondents most commonly reported that their organization was local in geographic scope by a wide margin (82%, N=162).

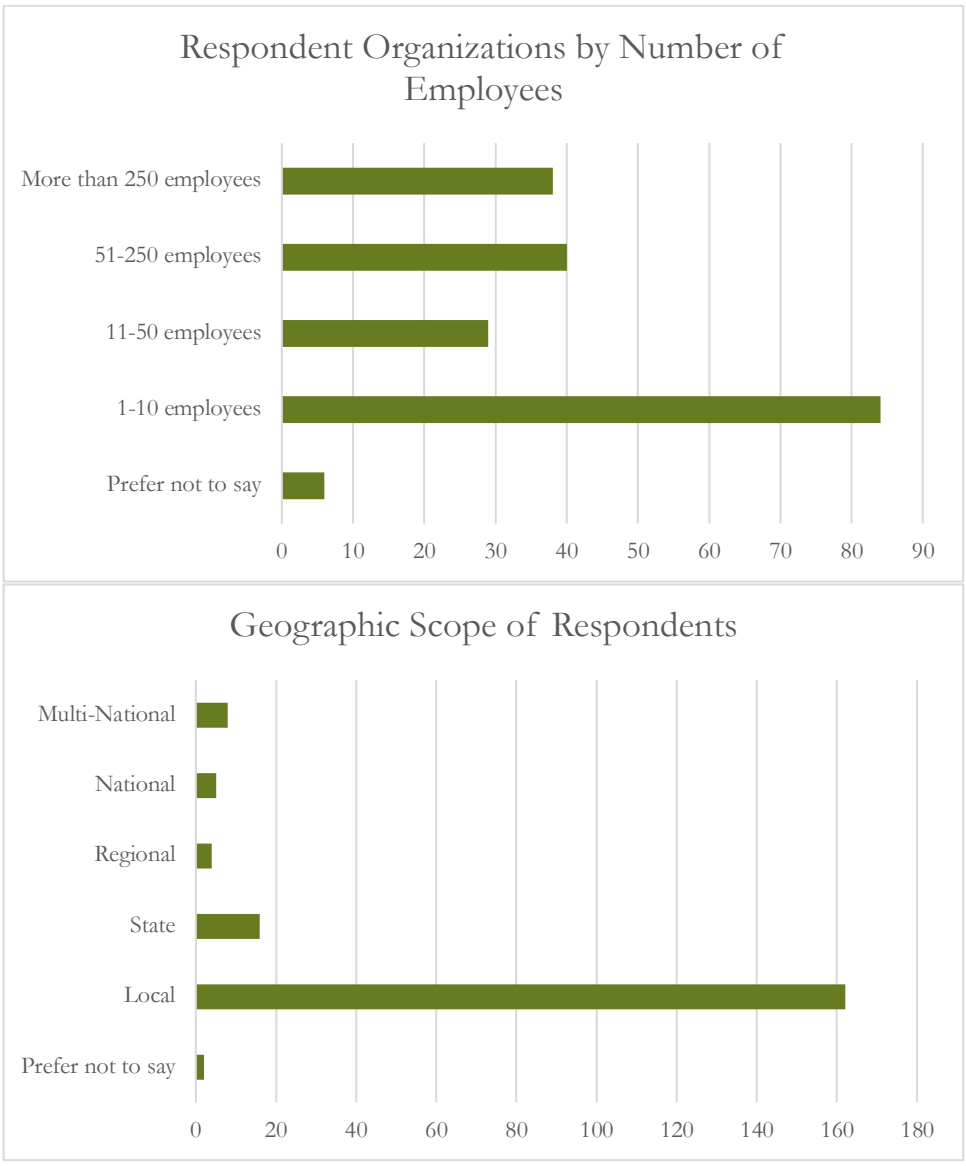



**Figure 3: Description of Respondent Organizations**

As there are particular concerns about cybersecurity decision-making amongst organizations that comprise critical national infrastructure, respondents were also asked whether their organization fell within one of these categories. As is shown in Figure 4 below, about 58% of respondents indicated that their organization fell within a critical infrastructure sector. In particular, about 36% of respondents reported that their organization fell within the Government Facilities Sector.

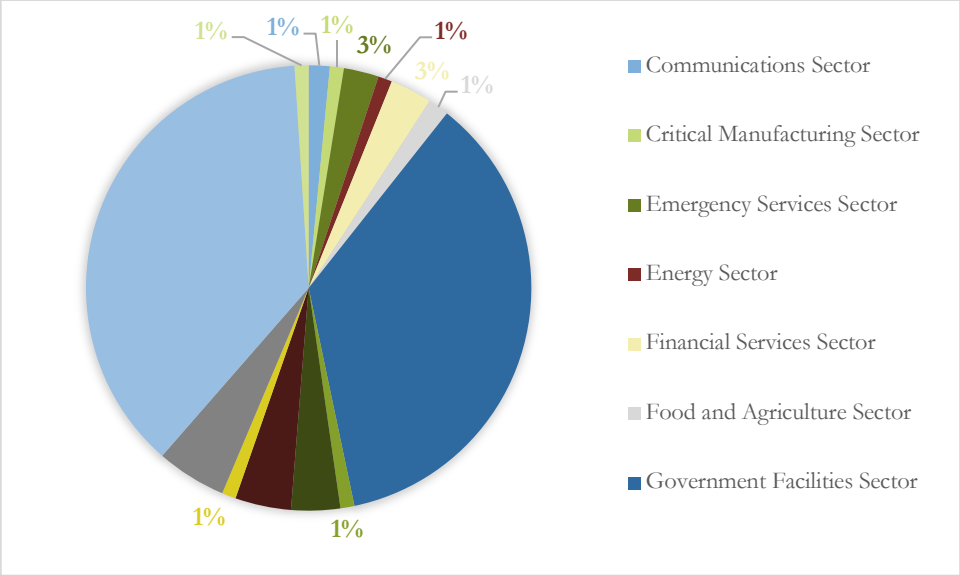



**Figure 4: Respondents by Critical Infrastructure Sector**

# C. Limitations

There are several key limitations to this analysis. It may be that cybersecurity decision-making amongst organizations that chose to respond to this survey may be different from those organizations that did not chose to respond. In particular, representatives from organizations that are more concerned about cybersecurity decision-making may be more likely to respond to the survey, as the issues it raises are more salient to them and their employers. Combined with the relatively low response rate of the survey, this suggests that the results of this analysis should not be seen as representing the exact parameters of cybersecurity decision-making in general. Rather, it should be seen as an exploratory effort to understand the range of factors that might contribute to cybersecurity decision-making in Indiana. Additionally, responses to the survey will be influenced by how respondents interpreted the questions, as well as the scope of their knowledge of their organization's cybersecurity practices and their recollection of these practices. Future, more in-depth qualitative research with organizations could provide additional details and insights that would refine the insights from this paper.

Nevertheless, this analysis can provide key insights to inform cybersecurity policymaking in Indiana today. It provides a description of mechanisms used by organizations to protect their information and mitigate potential attacks, which can be used to identify practices currently employed by organizations in the state. It explores the reasons why these practices have not been adopted, which can provide insights about barriers that governmental organizations may seek to address.

# Results

In this section, we summarize and discuss the responses provided by the Indiana organizations that participated in our survey. We focus specifically on describing cyber risk perceptions, planning, and responses. When possible we contextualize these responses with reference to other sources of data.

## A. Risk Perceptions & Experiences

### 1. Potential Events & Consequences

The Indiana organizations who responded to this survey generally expressed concern about the risk of a cyber incident. Almost 49% identified as very concerned and over 46% of respondents identified as somewhat concerned about the risk of a cyber incident, while less than 5% of respondents indicated that they were not at all concerned about the risk of a cyber incident. As shown in Figure 5 below, when asked about the specific types of cyber incidents they were concerned about, respondents most frequently indicated concern about malware attacks (86% of respondents), phishing attacks (76% of respondents), and ransomware attacks (74% of respondents). Of those respondents who indicated that they were concerned about another type of cyber incident, the types of incidents they described included zero-day exploits, attacks through third party vendors, and an attack that resulted in the release of client/patron information.

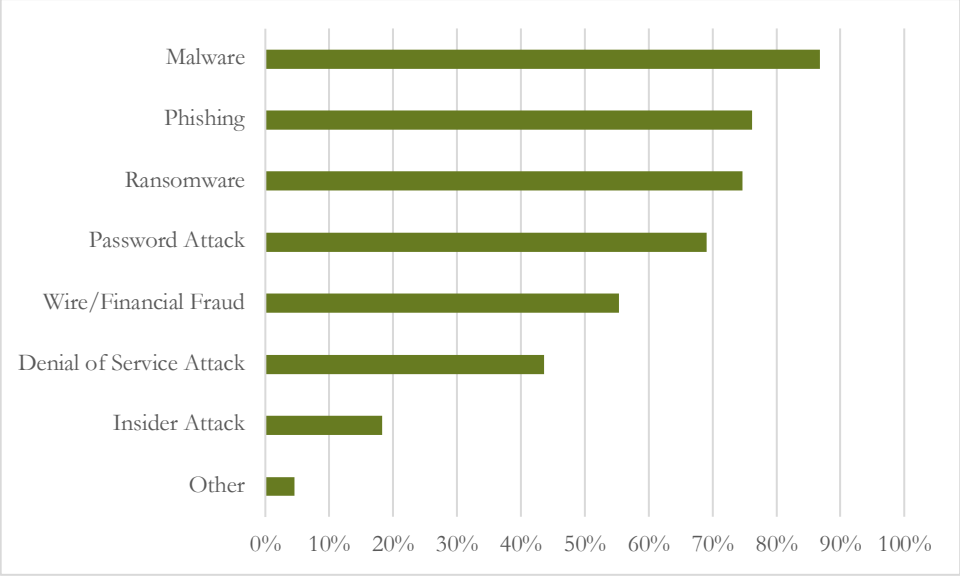



**Figure 5: Proportion of Respondents Concerned About Cyber Incidents, By Type**

Respondents were also asked to rank the types of cyber incidents they were concerned about in order of how concerned they were. Ransomware attacks were most commonly ranked as the highest concern amongst respondents who provided an answer to this question, while phishing attacks and malware attacks were ranked second and third respectively. Notably, respondents least frequently ranked insider attacks and other types of attacks as their highest source of concern, despite the overall prevalence of these issues.

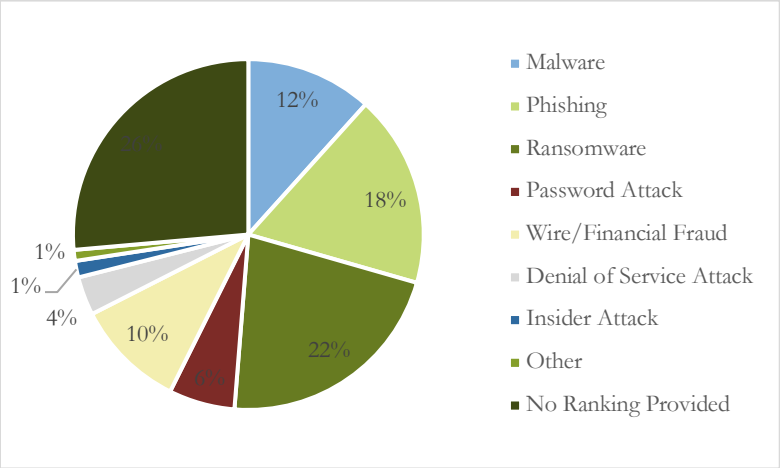



**Figure 6: Proportion of Respondents Most Concerned About Each Type of Cyber Incident**

In order to situate these results, we can compare them with data on data breaches reported to the Indiana Attorney General's office pursuant to Indiana's data breach notification statute in 2018 and 2019.[39] According to these data, the majority of data breaches reported to the Indiana Attorney General were caused by an external cause, as is shown in Figure 7 below.[40] The next most common cause of a reported data breach – inadvertent disclosure – occurred about a third as often as an external system breach. Reported data breaches were attributed to insider wrong-doing in about 6% of reported data breach. These results roughly align with concerns expressed by our respondents, who both most frequently mentioned external causes of cyber incidents such as malware and phishing attacks as potential sources of concern and ranked these external causes of cyber incidents as their sources of greatest concern.

[39] Ind. Code. Ann. § 24-4.9.

[40] The data used in this figure were obtained from public records of Notice of Security Breach Reports for Indiana. Simplified published versions of these reports are available at Indiana Attorney General, *Identity Theft Protection*, https://www.in.gov/attorneygeneral/2874.htm (last visited Oct. 29, 2020).

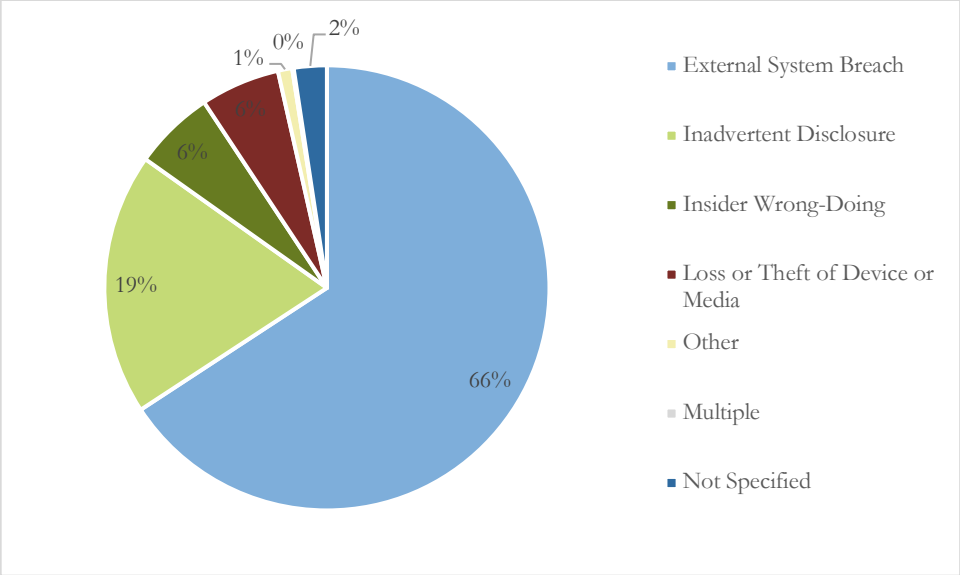



**Figure 7: Causes of Data Breaches Reported to the Indiana Attorney General**

Respondents were then asked about their concerns regarding the potential consequences of a cyber incident. As is shown in Figure 8 below, respondents most frequently indicated that they were concerned about data being deleted or lost (78% of respondents), data or information being exposed to outsiders (65% of respondents), and identity theft (64% of respondents). Interestingly, only a small proportion of respondents indicated that they were concerned with other potential consequences of a cyber incident. These respondents specifically indicated that they were concerned about personally identifying information being used against their stakeholders, and the loss of resources and staff time incurred in the course of responding to the incident.

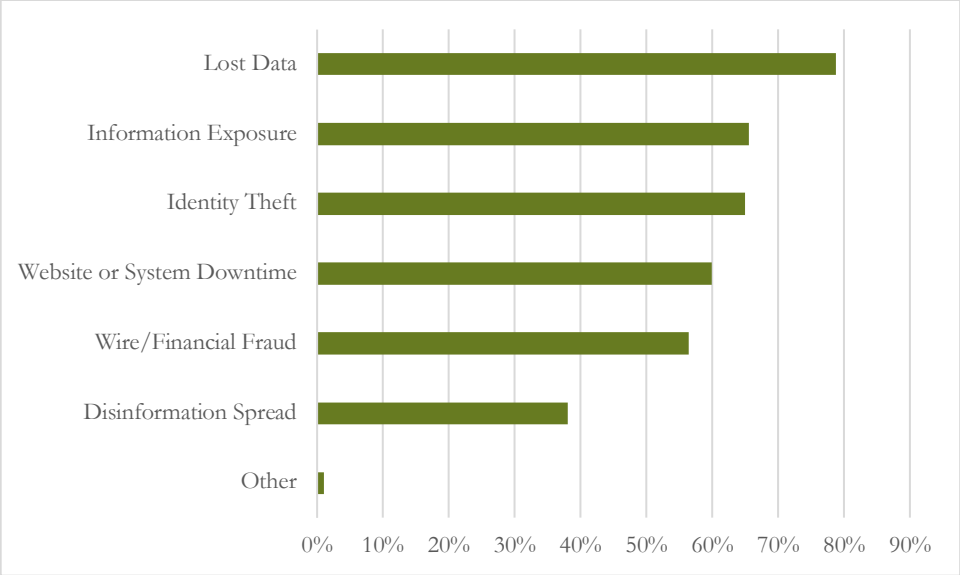



**Figure 8: Proportion of Respondents Concerned About Consequences of Cyber Incidents, By Type**

Respondents were again asked to rank the potential consequences of cyber incidents based on their level of concern. Of those who provided an answer to this question, respondents most frequently indicated that they were most concerned about data being deleted or lost (22% of respondents), data being exposed to outsiders (16% of respondents), and wire/financial fraud (11% of respondents).

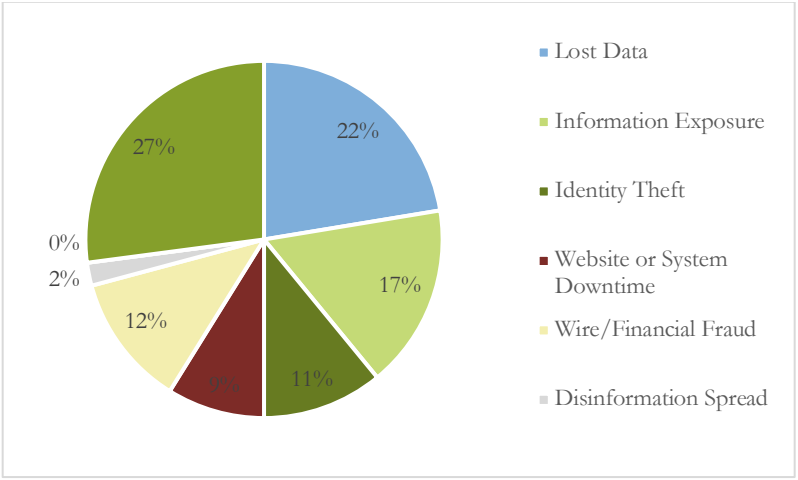



**Figure 9: Proportion of Respondents Most Concerned About Consequence of Cyber Incident**

## 2. Previous Events and Responses

In order to understand Indiana organizations' previous experiences with and responses to cyber incidents, respondents were asked whether their organization had experienced a successful cyber incident in the past three years. Approximately 19% (N=38) of respondents indicated that they had experienced a successful cyber incident during this time frame, while 67% (N=132) of respondents indicated that their organization did not experience a successful cyber incident and 13% (N=25) were either not sure or declined to provide an answer. Of respondents who indicated that their organization had experienced a successful cyber incident in the past three years, 50% indicated that none of these incidents resulted in data loss and 31% indicated that less than five of these incidents resulted in data loss. Respondents were then asked to describe the most recent incident experienced by their organization. As is shown in Figure 10 below, the most common types of cyber incidents experienced by respondents were phishing attacks and wire/financial fraud, while no respondents indicated that the most recent incident experienced by their organization was a DDoS attack.

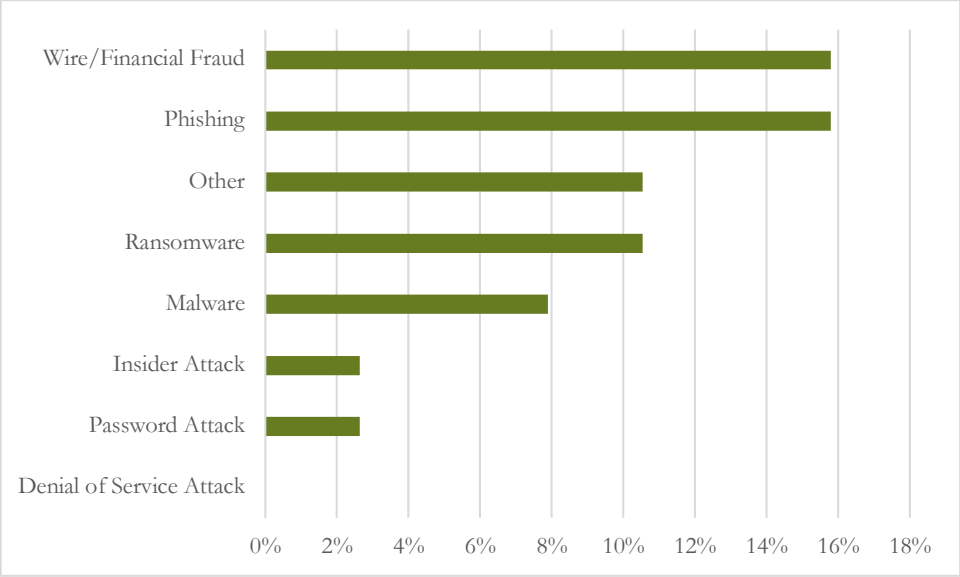



**Figure 10: Types of Cyber Incidents Experienced by Respondents' Organizations**

Respondents also described the consequences of the most recent cyber incident experienced by their organization; these results are summarized in Figure 11 below. Over 18% (N=7) respondents reported experiencing exposure of information to outsiders as a result of the cyber incident, while over 15% (N=6) reported wire/financial fraud as a result of the cyber incident.

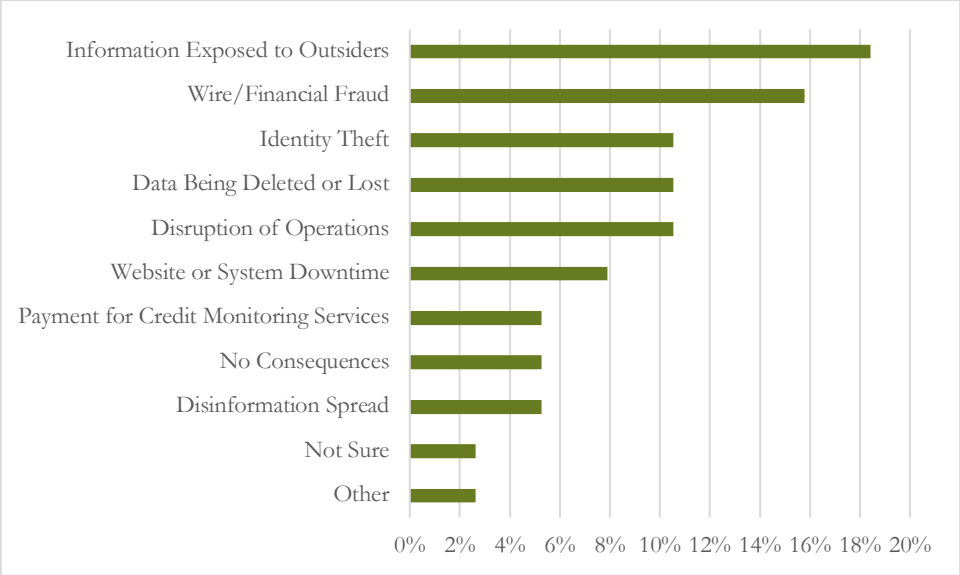



**Figure 11: Consequences of Cyber Incidents Experienced by Respondents' Organizations**

# B. Managing Cyber Risk

## 1. Prevention and Mitigation of Cyber Incidents

Prevention is a key component of an effective cybersecurity strategy. The vast majority – over 82% – of respondents indicated that their organization had taken steps to prevent a cyber incident; over 7% indicated that their organization had *not* taken steps to prevent cyber incidents, and over 9% indicated that they were not sure. Of respondents who indicated that they had taken steps to prevent cyber incidents, there was a high degree of commonality in the mechanisms adopted. As shown in Figure 12 below, over 95% of respondents who indicated that they had taken steps to prevent cyber incidents installed antivirus software (N=155), while over 75% (N=126) indicated that they had updated/patched software and over 70% (N=114) provided their employees with training to reduce cyber-related risks. Seventeen respondents indicated that they had used mechanisms to prevent cyber incidents other than the options provided by the survey; these respondents described a broad range of alternative mechanisms including installing firewalls and spam filters, adopting multi-factor authentication, and hiring a cybersecurity firm to advise on defenses.

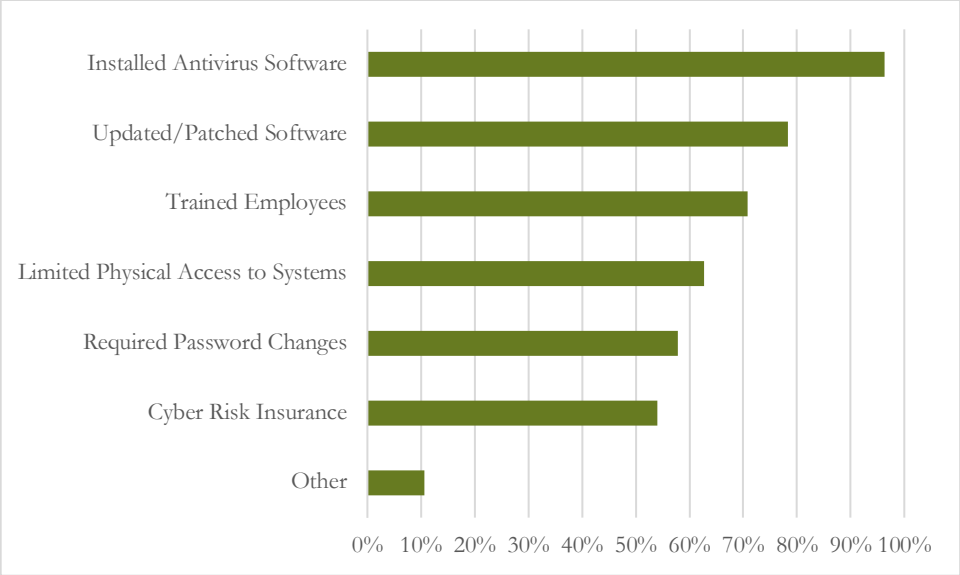



**Figure 12: Mechanisms Used to Prevent Cyber Incidents**

Respondents who indicated that their organization had not taken steps to prevent cyber incidents were then asked why these steps had not been taken. As shown in Figure 13 below, of those respondents who indicated that their organization had not taken steps to adopt cyber incident prevention mechanisms, slightly more than half (N=8) attributed this decision to the organization being unsure what to do, while 40% (N=6) explained that their organization did not think it was at risk. Twenty percent (N=3) indicated that their organization had reasons other than those provided by the survey for not adopting cyber risk prevention mechanisms; these respondents generally went on to explain that their organization was either too small to engage in prevention mechanisms or did not have their own equipment to protect. Perhaps most interestingly, no respondents indicated that their organization did not adopt cyber incident prevention mechanisms because they believed those mechanisms to be ineffective.

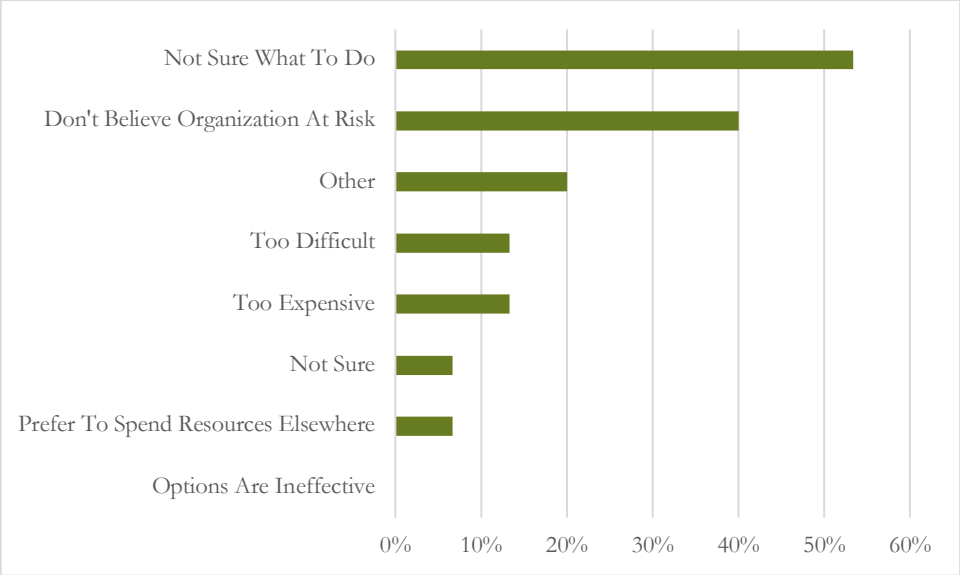



**Figure 13: Reasons for Not Adopting Prevention Mechanisms**

Almost 70% (N=134) respondents indicated that their organization had taken steps to mitigate the impact of a cyber incident, while about 11% (N=23) indicated that their organization had not taken these steps and about 19% (N=37) were not certain. Respondents who indicated that their organization had adopted mechanisms to mitigate cyber incidents were then asked what mitigation mechanisms their organization had undertaken. As is shown in Figure 14 below, almost 85% (N=113) of respondents indicated that their organization had installed automatic back-up systems, while approximately 60% (N=84) of respondents indicated that their organization had purchased cyber risk insurance. Almost 12% (N=16) of respondents described other cyber incident mitigation mechanisms undertaken by their organization; such mechanisms included upgrading hardware, strengthening firewalls, and testing their network or incident response plan.

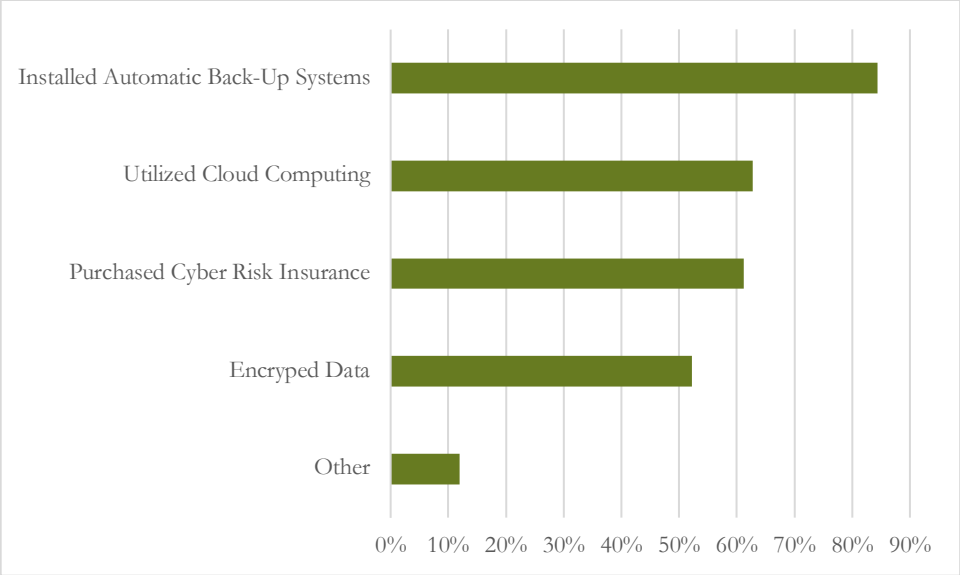



**Figure 14: Mechanisms Used to Mitigate Cyber Incidents**

Respondents who indicated that their organizations had not adopted mitigation measures were then asked why these measures had not been adopted. Respondents most commonly cited uncertainty about how to accomplish this as the reason their organization had not adopted mitigation mechanisms, with about 47% (N=11) respondents adopting this option. Twenty-six percent (N=6) of respondents indicated that their organization had not adopted mitigation mechanisms because they didn't believe themselves to be at risk. The approximately 17% (N=4) of respondents who characterized their organization as having other reasons for not adopting mitigation mechanisms elaborated that these reasons included not having technical infrastructure to secure or currently being at the stage of investigating mitigation options.

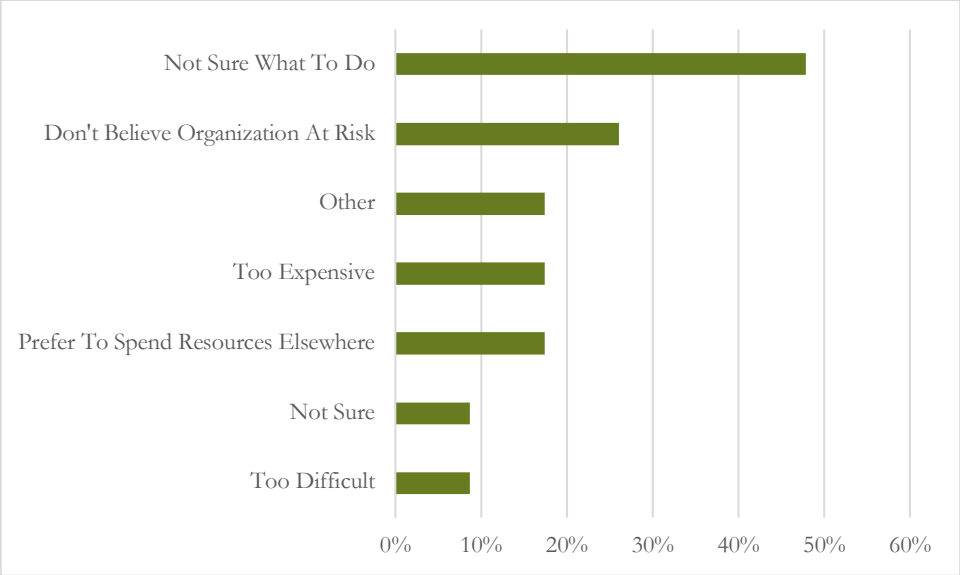



**Figure 15: Reasons for Not Adopting Mitigation Mechanisms**

## 2. Cybersecurity Practices, Personnel, and Training

In order to understand how Indiana organizations are protecting their systems and information, respondents were then asked whether their organization had adopted certain cybersecurity practices. As is shown in Figure 16 below, of the 178 respondents who answered the question, slightly less than half indicated that their organization had adopted automatic updating of operation systems and software (N=88) and implementation of remote backups (N=86). The next most commonly adopted practice was use of multi-factor authentication, which about a quarter of respondents had indicated that their organization had adopted.

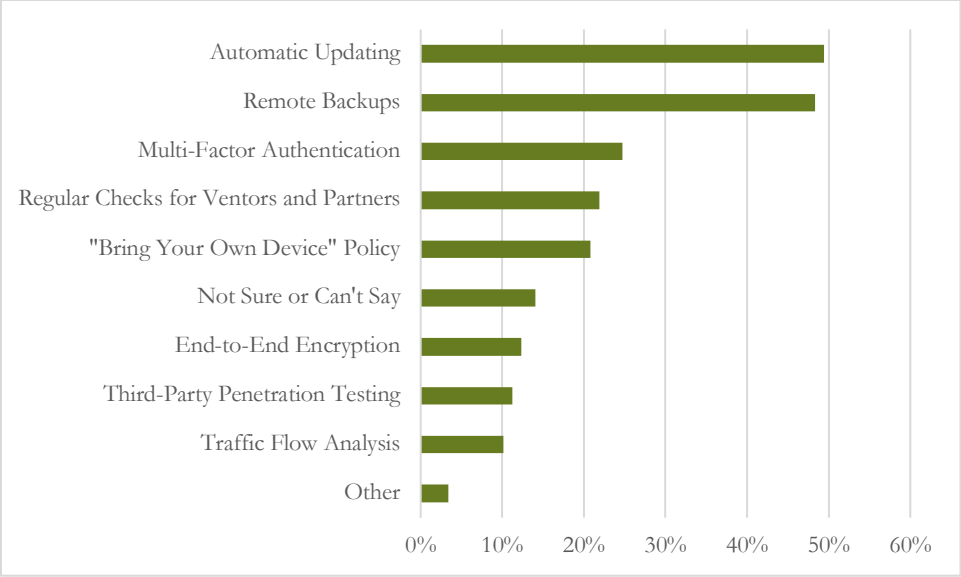



**Figure 16: Cybersecurity Practices Adopted**

The development and documentation of incident planning and response is a key cybersecurity practice. About 27% (N=55) of respondents reported that their organization had written cyber incident planning and response documentation, with more than half (N=109) indicating that their organization did not have such documentation and the remainder of respondents being uncertain or unresponsive. Respondents who indicated that their organization had written cyber incident planning and response documentation were then asked about their perceptions of the documentation. As shown in Figure 17 below, these perceptions were weakly positive on average, with respondents on average falling between “somewhat agree” and “neither agree or disagree” for all statements. However, there was a degree of polarization in these responses, with “strongly agree” being the most frequently occurring response to all statements.

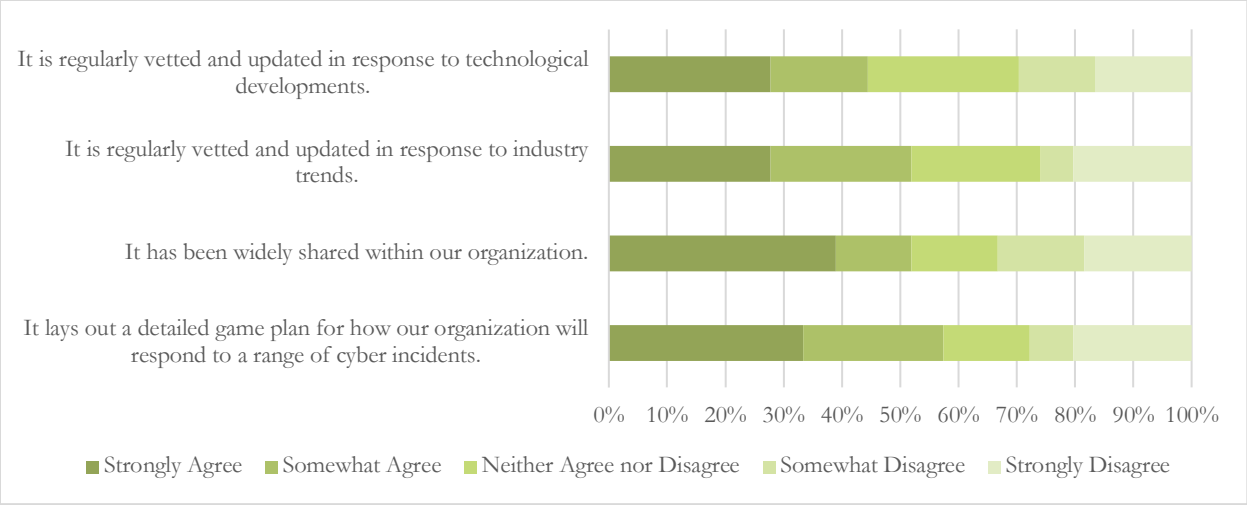



**Figure 17: Perceptions of Cybersecurity Documentation**

Cybersecurity response is also shaped by the people selected to lead this response. When asked who at their organization was ultimately responsible for managing cyber risk, about 15% (N=30) of respondents indicated this role was filled by their Chief Information Officer, and about 14% (N=28) indicated that this role was filled by their Chief Executive Officer. Interestingly, almost half of respondents elected to write in their own response to this question, with a common response being that this role was fulfilled by an information technology manager, director, or department (and several respondents indicating that no one served in this role). The heterogeneity of these responses suggests that many Indiana organizations seek guidance about corporate governance best practices to ensure that cybersecurity and data privacy are adequately integrated into organizational decision-making.

Respondents were also asked how many cybersecurity professionals were employed at their organization. Sixty-seven percent (N=133) indicated that their organization did not employ a cybersecurity professional, and 23% (N=47) indicated that their organization employed between 1 and 5 cybersecurity professionals. Additionally, as all employees can play a role in ensuring an organization's cybersecurity, respondents were asked about cybersecurity training practices at their organizations. While 58% (N=116) indicated that their organization had provided some employees with cyber risk awareness training, only 29% (N=58) of respondents stated that they themselves had received such training. A plurality of respondents who received such training (44%, N=25) stated that they received yearly training, while a smaller minority (32%, N=18) stated that their received training once a quarter.

## 3. Usefulness of Standards & Frameworks

A proactive approach to cybersecurity includes preemptively identifying security weaknesses and adding processes to identify threats before they occur. However, a plurality of respondents (37%, N=69) were not sure whether their organization was using specific tools to proactively manage cyber risk. Thirty-four percent (N=32) indicated that their organization had revised or

updated their incident response plan, while 32% (N=60) indicated that their organization had consulted news reports to proactively manage cyber risk. The 8% (N=16) of respondents who stated that their organization had taken other steps to proactively manage cyber risk described that these steps included having their computer system audited and hiring a consultant for monitoring.

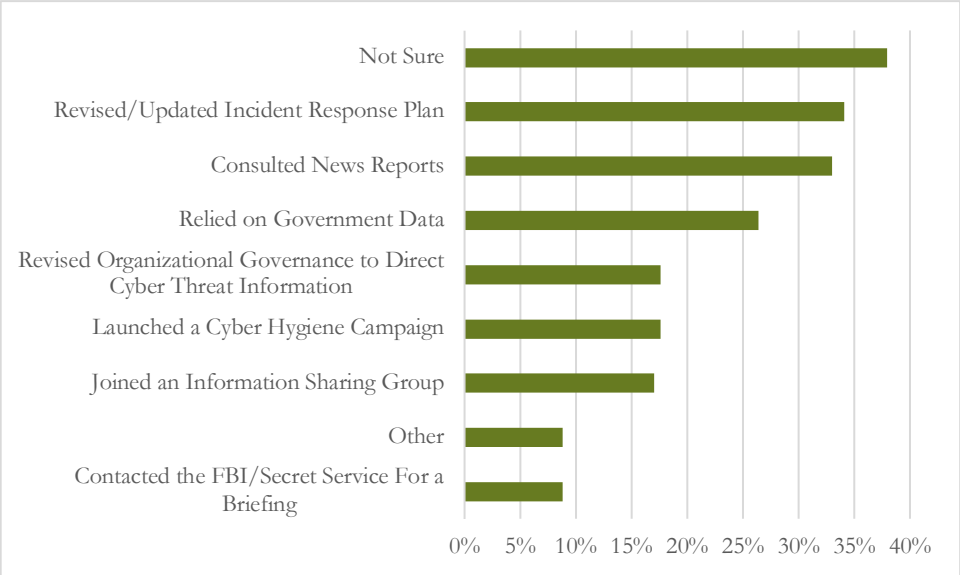



**Figure 18: Tools Used to Proactively Manage Cyber Risk**

Organizations concerned about their cybersecurity have a range of external tools and frameworks available to help guide their decision making in this area. Fifty-eight respondents (29%) stated that their organization consulted an externally developed tool, framework, or control when making decisions about cyber practices. Among respondents who indicated that their organization used an externally developed framework to guide their cybersecurity decision making, the most commonly used framework was the NIST Cybersecurity Framework, which had been adopted by 58% (N=34) of those organizations adopting a framework and 36% (N=21) had adopted the Center for Internet Security (CIS) Critical Security Controls.

# C. Role of Cyber Risk Insurance

About half of respondents (N=98) indicated that their organization had cyber risk insurance; 26% (N=52) indicated that their organization did not have cyber risk insurance; remaining respondents (N=47) were either unsure or declined to answer. In this section, we explore how organizations with cyber risk insurance decided to obtain this insurance coverage, what is covered under these policies, and what is required by these policies.

## 1. Adoption of Cyber Insurance

Respondents with knowledge of when their organization had obtained cyber risk insurance most frequently indicated that this insurance had been obtained within the last five years, as indicated in Figure 19 below. Interestingly, one respondent indicated that their organization had obtained cyber risk insurance in 2001, almost a decade before any other respondent.

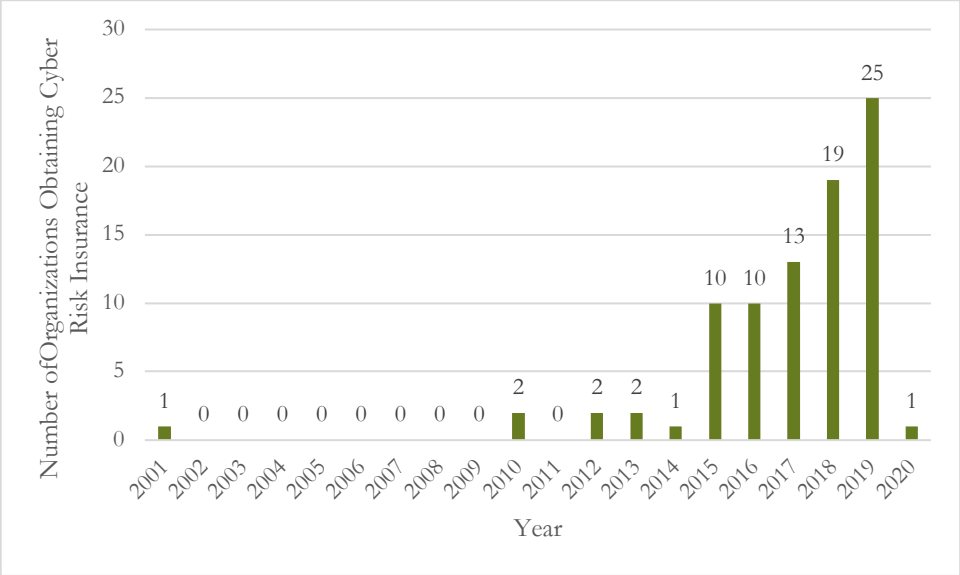



**Figure 19: Year Cyber Risk Insurance Was Obtained**

Respondents were then asked why their organization obtained a cyber risk insurance policy; the results of this question are described in Figure 20 below. Half of respondents (N=49) described the decision to obtain cyber risk insurance as a response to news reports on cyber incidents. A large minority (40%, N=40) of respondents provided another reason for obtaining cyber risk insurance. These reasons included insurance agent recommendations or inclusion of cyber coverage in a general policy,[41] response to cybersecurity trainings by trade organizations or other outside groups, and a perception that obtaining this insurance "just made business sense."

[41] As coverage provided under a general policy might be different than coverage provided under a cyber-specific insurance policy, these responses could raise concerns about an additional source of insurance policy variation amongst respondents. However, as only three respondents indicated that their organization obtained cyber insurance as part of a more general policy, these responses have probably not had an outsized influence on our overall analysis.

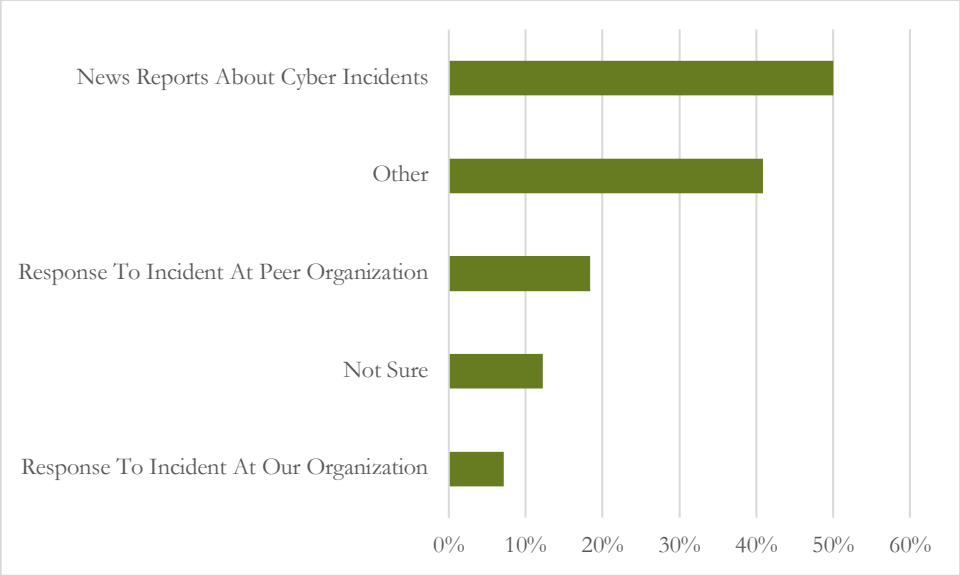



**Figure 20: Reasons for Obtaining Cyber Risk Insurance**

## 2. Cyber Insurance Coverage

Cyber insurance plans may offer coverage for incidents that occur under a variety of circumstances, and losses that occur to a variety of people and organizations. Insurance plans commonly cover first-party losses, which are losses that are incurred by the insured. Figure 21 below describes the first-party losses covered by respondent organizations' insurance plans. In particular, respondents whose organizations had cyber risk insurance most commonly reported that their organization's insurance policy covered losses due to damage to computers or information systems (54%, N=53), with a similar but slightly smaller number of respondents indicating that their organization's cyber insurance policy covered expenses related to responding to the breach (52%, N=51).

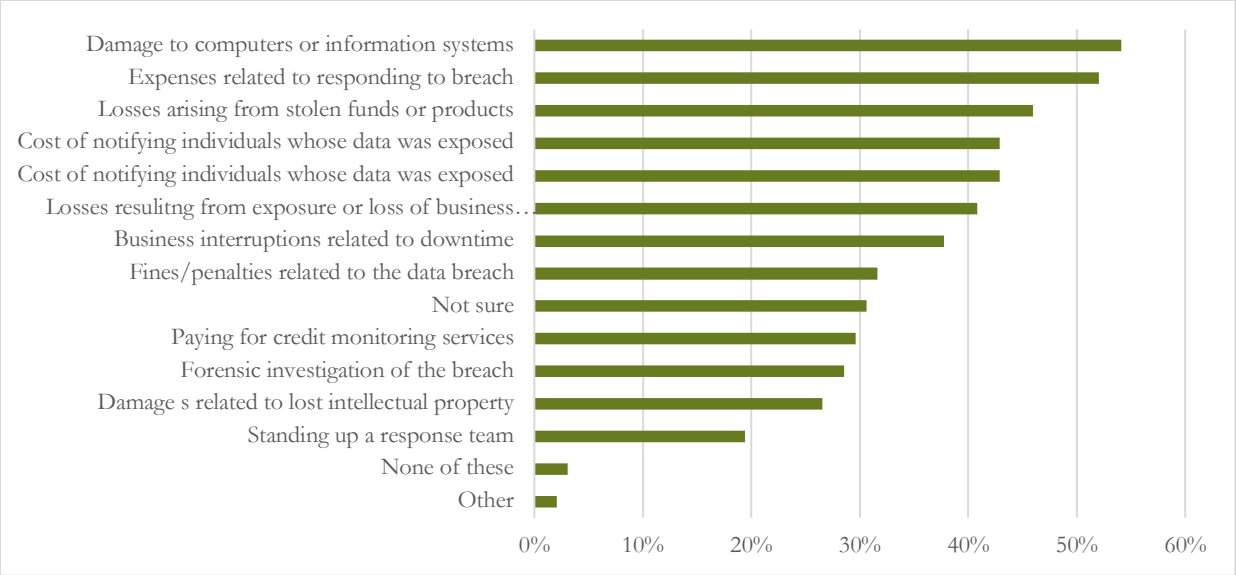



**Figure 21: First Party Losses Covered Under Cyber Insurance**

In addition to first party losses, cyber insurance plans may also cover third-party losses, which are losses incurred by other parties for which the insured party may nonetheless be liable. As is shown by Figure 22 below, respondents were less sure about the third-party losses covered under their organization's cyber insurance policy. However, about 33% (N=33) of respondents whose organizations have cyber risk insurance policies reported that this policy included costs for legal defenses related to the data breach, while about 26% (N=26) reported that this policy included coverage for claims for damages from those whose information was exposed by the incident.

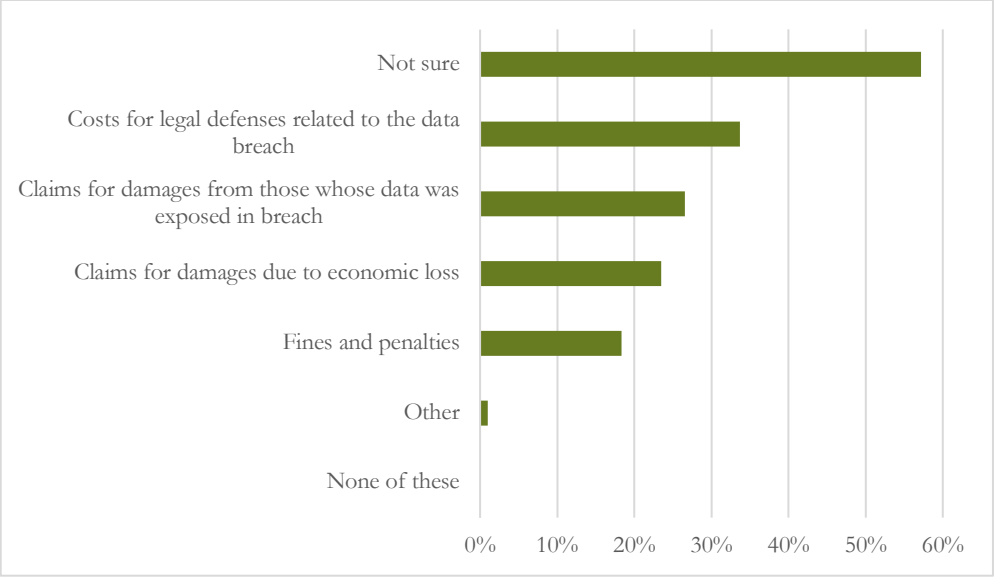



**Figure 22: Third Party Losses Covered Under Cyber Insurance**

Over 60% (N=59) of respondents with cyber insurance policies reported that these policies included a limit on coverage; the remainder were largely unsure as whether their policy included such a limit. Out of the 35 respondents who reported the amount of their coverage limit, the most commonly reported limit was $1 million; however, some respondents reported a coverage limit in the hundreds of millions of dollars. In addition to limitations on coverage amount, insurers may also exclude certain categories of incidents from coverage under a policy. The majority of respondents who indicated that their organization had insurance coverage were unsure as to whether that insurance policy excluded coverage in certain circumstances, although almost 20% (N=18) of respondents whose organizations had cyber risk insurance reported that this policy had coverage exclusions. Of those respondents who were able to provide information about these exclusions, the most frequently cited reason for exclusion was acts of war or terrorism, with losses that occurred because the organization failed to provide and maintain adequate security.

## 3. Required Security Measures

As insurers bear risks associated with potential cyber incidents, it is common for cyber risk insurance policies to require the insured organization to undertake certain security practices. Of those respondents who indicated that their organization had a cyber risk insurance policy, 47% of them indicated that this policy required them to undertake certain security measures. As is shown in Figure 23 below, the most commonly required security practices were employee training and cyber hygiene, with about 40% (N=19) of those whose organizations were required to adopt security practices by their insurer indicating that these required practices included employee training. About 34% (N=16) indicated that their insurer required their organization to engage in mandatory, automatic patching of systems. Respondents who indicated that their insurer required other security measures were asked to describe these security measures.

Responses included the development of a cybersecurity plan and compliance with the Payment Card Industry Data Security Standard.

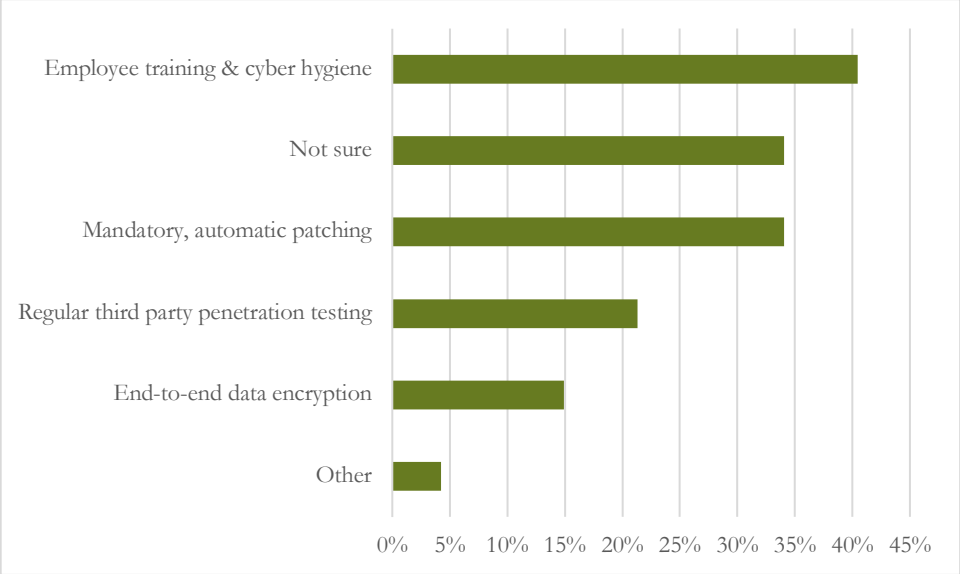



**Figure 23: Security Measures Required by Respondents' Insurer**

## 4. Non-Adoption of Cyber Risk Insurance

Policymakers and analysts interested in understanding cyber risk insurance decision-making can learn just as much from organizations that do not have cyber risk insurance as from those who do. Consequently, respondents whose organizations did not have a cyber risk insurance policy were asked whether their organization had ever considered obtaining a cyber risk insurance policy and, if so, why they did not decide to obtain such a policy. Almost half (48%; N=46) of respondents whose organizations did not have a cyber risk insurance policy indicated that their organization had never considered obtaining such a policy, while 38% (N=37) indicated that they were unsure. About 13% (N=12) indicated that their organization had considered obtaining such a policy and had decided against it. These respondents most commonly indicated that cost was a factor in the decision not to obtain cyber risk insurance, either because they believed it to be too expensive or their preferred to spend resources on other policies. One respondent who provided an additional reason that their organization had not adopted a cyber risk insurance policy indicated that their organization may have been "overwhelmed with what exactly we really needed to obtain."

Respondents who did not currently have cyber risk insurance were asked what would encourage their company to obtain a cyber risk insurance policy as an open-ended question. Responses unsurprisingly covered a range of potential factors. Many respondents described the cost of obtaining a policy as a significant factor, frequently mentioning affordability and the need for "a better value proposition." Other respondents indicated that their organization would be more likely to obtain cyber risk insurance if they perceived they were more at risk ("awareness of the treat and the damage that could result"), or if they obtained additional information about their

level of risk either through incidents at peer organizations or general statistics. Finally, some respondents indicated that their organizations were unlikely to ever obtain cyber risk insurance, generally due to the fact that they did not perceive that their organization was ever likely to be at risk.

# Policy Opportunities

## A. Awareness Training

As was made clear in our results, there is a clear need to help educate organizations about cybersecurity best practices with more than half of respondents being unsure of which techniques and tools to use to best mitigate the particular cyber risks they face. In particular, given concerns over malware, phishing, and ransomware, public-private training sessions would seemingly be well suited to focus on these issues in particular. Indiana has made strides in this regard such as through the Indiana Cybersecurity Hub,[42] and the Indiana Information Sharing and Analysis Center (IN-ISAC).[43] However, greater coordinated outreach by leveraging educational institutions, civil society groups, and law enforcement could address this lack of awareness potentially through a push to promote October as Cybersecurity Awareness Month. Senior leadership in particular, including boards of directors, should be a key area of focus given the diffusion of cybersecurity responsibilities and persistent lack of clarity about accountability at so many Indiana organizations.

A concrete idea that the Executive Council could consider to help address this clear need is by working with universities and community colleges across the state to create a cybersecurity curriculum that local and state leaders could access and would answer these questions, such as best practices for ransomware mitigation. The site could also include model incident response plans, explainers for cyber risk insurance coverage and common exclusions, and other tools. Relatedly, we would encourage a deeper partnership – perhaps in collaboration with regional economic development authorities, the IN-ISAC, and the Indiana Business Research Center – between state and local leaders on quarterly trainings on various cybersecurity hot topics such as ransomware and the need to enable multi-factor authentication, end-to-end encryption for sensitive databases, and BYOD policies.

## B. Proactive Cybersecurity

As seen in the results to this survey, while many organizations (82% of respondents) have taken some steps to prevent a cyber incident mostly through investing in antivirus solutions and patching, it is not uncommon to maintain a reactive cybersecurity stance across Indiana organizations. Proactive cybersecurity is an amorphous field, comprising a wide range of active and passive measures that are often commonly, though not always accurately, referred to as "active defense." While "hacking back" is a lightning rod within this field,[44] it is just one data

[42] *See* Indiana Cybersecurity Hub, https://www.in.gov/cybersecurity/ (last visited Oct. 1, 2020).

[43] IN-ISAC, https://www.in.gov/cybersecurity/in-isac/ (last visited Oct. 1, 2020).

[44] *See, e.g.*, Carl Franzen, *Should US companies be allowed to hack China in revenge? New report says yes*, VERGE (May 22, 2013), http://www.theverge.com/2013/5/22/4356196/report-tells-congress-companies-should-hack-back [https://perma.cc/JX7X-FE7X]; *see also* Eric Chabrow, *The Case Against Hack-Back*, BANK INFO. SEC.

point in a larger and more dynamic movement, which includes technological, organizational, and legal best practices deep packet inspection to audits promoting defense-in-depth.[45] Such a "lean in" approach to cybersecurity is essential to help guard against the more reactive mindset that has long bedeviled the field of cybersecurity risk management.[46] There seems to be an opportunity to help educate Indiana organizations about the full range of proactive cybersecurity best practices available to them to help manage various cyber risks. This can include both spreading awareness of, and encouraging the uptake including through government procurement, of leading cybersecurity and privacy frameworks including from NIST. Although this was the dominant option selected by respondents, still more than 40% of Indiana participants are not utilizing it at present. The proposed 2020 IN Attorney General's cybersecurity rule, discussed next, would constitute such a nudge.[47]

## C. Defining "Reasonable" Cybersecurity

On September 25, 2020 Indiana Attorney General Curtis Hill proposed a rule that would change the incident response process for Indiana organizations that have experienced a data breach. In brief, the proposal would make two main substantive revisions from the current structure: (1) impose a requirement for database owners to "create, implement and report a corrective action plan (CAP) to the Attorney General within thirty days" of the reported breach; and (2) establish "a 'safe harbor' for what constitutes 'reasonable measures' to safeguard personal information in Indiana."[48] Database owners are those persons or entities that "own or license computerized data that include personal information."[49] Under existing Indiana law, these owners should "implement and maintain reasonable procedures, including taking any appropriate corrective

---

(Jan. 6, 2015), http://www.bankinfosecurity.com/case-against-hack-back-a-7759 [https://perma.cc/9WXW-U7TK]; Tom Field, *To 'Hack Back' or Not?*, BANK INFO. SEC. (Feb. 27, 2013), http://www.bankinfosecurity.com/to-hack-back-or-not-a-5545 [https://perma.cc/7XUH-H8T9] (discussing, among other things, the likelihood of prosecution in the United States for engaging in hacking back).

[45] *See, e.g.*, Orla Cox, *Proactive Cybersecurity — Taking Control Away from Attackers*, SYMANTEC (Apr. 2, 2014), http://www.symantec.com/connect/blogs/proactive-cybersecurity-taking-control-away-attackers [https://perma.cc/3XM6-R369]; Michael A. Davis, *4 Steps for Proactive Cybersecurity*, INFO. WK. (Jan. 18, 2013), http://www.informationweek.com/government/cybersecurity/4-steps-for-proactive-cybersecurity/d/d-id/1108270 [https://perma.cc/8XYL-H3PN]; *Hackback? Claptrap! — An Active Defense Continuum for the Private Sector*, RSA CONF. (Feb. 27, 2014), http://www.rsaconference.com/events/us14/agenda/sessions/1146/hackback-claptrap-an-active-defense-continuum-for ("[A]ctive defense should be viewed as a diverse set of techniques along a spectrum of varying risk and legality.").

[46] MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 6 (2009), https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf [https://perma.cc/N6L4-KAML] (comparing cybersecurity investment rates across countries and concluding that "it appears that decision makers in many countries, particularly developed ones, are reactive rather than proactive").

[47] IN Attorney General Proposal Rule LSA Document # 20-366, https://www.workplaceprivacyreport.com/wp-content/uploads/sites/162/2020/09/IN-AG-Hill-Proposed-Regulations.pdf.

[48] *See* Joseph J. Lazzarotii, *Indiana AG Proposed Regulations Creating Corrective Action Plan Requirement and Cybersecurity Safe Harbor*, WORKPLACE PRIVACY REP. (Sept. 25, 2020), https://www.workplaceprivacyreport.com/2020/09/articles/data-breach-notification/indiana-ag-proposed-regulations-create-corrective-action-plan-requirement-and-safe-harbor/.

[49] *Id.*

action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner."[50] As Attorney General Hill said in describing the proposal: "This rule would provide businesses a playbook on how to protect data, and would protect the businesses that follow the playbook. It's a win for both consumers and businesses."[51]

A key piece of this effort is specifying what 'reasonable' cybersecurity entails. To date, that varies across the more than one dozen states with such laws on the books. Under Californian law, for example, organizations are required to implement "reasonable security procedures and practices . . . to protect personal information from unauthorized, access, destruction, use, modification, or disclosure."[52] The California Attorney General's Office defined "reasonable" to include the following list of Center for Internet and Security controls as the *minimum* threshold, which include requiring multi-factor authentication, and end-to-end encryption on portable devices.

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Security Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browsing Protection
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capability
11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

---

[50] *Id.*

[51] *Id.*

[52] Paul Otto & Brian Kennedy, "*Reasonable Security" Becomes Reasonably Clear to California Attorney General*, CHRONICLE OF DATA PROTECTION (Mar. 1, 2016), https://www.hldataprotection.com/2016/03/articles/cybersecurity-data-breaches/reasonable-security-becomes-reasonably-clear/.

Instead, the proposed Indiana rule mirrors the efforts from other Midwestern states including Ohio's safe harbor law and offers a list of leading cybersecurity frameworks that, if adopted, are presumptively reasonable. These include: the aforementioned NIST CSF, ISO 27000, along with sector-specific laws depending on the sector and industry in which the covered entity is operating, which could include the Fair Credit Reporting Act, Health Insurance Portability and Accountability Act (HIPAA), and/or the payment card industry data security standard (PCI). There are also proposed requirements for regular improvements, such as by implementing up-to-date versions of the NIST CSF, timely tracking vulnerabilities and applying remediation strategies, and updating incident response plans at least annually.

## D. Incident Response Best Practices

Under the proposed 2020 Indiana AG cybersecurity rule, covered entities may need to take steps to amend their incident response plans to submit a CAP within a timely fashion (e.g., within thirty days). This requirement would help address the demonstrated lack of planning as seen in the results of this survey with only 27% of respondents reporting that their organizations had a written incident response plan on file. Requirements built-in to the proposed rule to ensure that such plans are regularly updated (e.g., at least annually) could help address this shortfall. Additional steps to aid in this process, and dovetailing with the need for better cyber awareness, would be to encourage that such plans are widely communicated, and even vetted by third parties including insurance firms. The Executive Council could work with universities and other partners to coordinate regular incident response and tabletop exercises to highlight the importance of this proactive planning. One idea would be to focus on one critical infrastructure sector roughly each month, and then conduct a follow-up survey to see how practices have changed after the trainings have taken place.

## E. Cyber Risk Insurance

As is evident from this survey, there remains significant barriers for Indiana organizations accessing this tool, including cost, awareness, and confusion over coverage for both first and third-party losses. Given that only 20% of the survey respondents likewise were aware of exclusions in their policies, it seems clear that the State has a role to play in helping Indiana organizations navigate what types of cyber risks insurance can, and cannot, help mitigate. One tool to help in this regard, which could be folded into Indiana's Cybersecurity Hub offerings, could take the form of a guide modeled after Citizen Lab's *Security Planner* but focused not just on cybersecurity best practices, but also on the navigating cyber risk insurance questions across markets, and sectors.

We plan follow-up surveys to periodically assess how Indiana is improving along these metrics, and hope that these results help convince other states to follow Indiana's example in this regard.

# Appendix A: Sources Used for Figure 1

- **State Phishing** - https://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx
- **Ransomware & DDOS** - https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#Ransomware
- **Spyware** - https://www.ncsl.org/research/telecommunications-and-information-technology/state-spyware-laws.aspx
- **Cybersecurity Taskforce** - https://www.ncsl.org/research/telecommunications-and-information-technology/statewide-cybersecurity-task-forces636129887.aspx
- **Cybersecurity interest** - https://www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf

# Appendix B: Indiana Cybersecurity Survey Protocol

---

Start of Block: Cyber Risk Perceptions

Q1.1
Cyber incidents - such as phishing attempts, malware attacks, and ransomware demands - are increasingly an area of concern for both the public and private sectors. Although organizations have options for managing cyber risk, relatively little is currently known about what steps are being taken, including what role insurance is playing in this planning process. Additional information would help identify barriers that prevent effective cyber risk planning, while enabling organizations to better understand how their cyber risk planning compares with that of their peers. To get a more complete picture of Hoosier cyber risk planning, the Legal and Insurance working group of the Indiana Executive Cybersecurity Council, in collaboration with researchers at Indiana University and the University of Arizona, is conducting a study to help explore how Indiana organizations perceive and manage cyber risks. This study will pay particular attention to the role of insurance as part of an overarching cyber risk mitigation strategy. The report resulting from this study will provide policymakers and law enforcement with important information about cyber readiness, and help Hoosier organizations like yours better understand current cyber practices in your industry.

We are asking you to participate in this study by filling out a short survey describing your organization's perceptions of cyber risk and use of cyber risk insurance. This survey will take no more than 25 minutes to complete. The responses you provide will only be reported in the aggregate. Your participation is entirely voluntary, and you would be free to terminate the survey at any point. Thank you very much.

Curtis T. Hill, Jr.
Indiana Attorney General Co-Chair of the Legal and Insurance working group of the Indiana Executive Cybersecurity Council

- I agree to participate in the survey
- I do not agree to participate in the survey

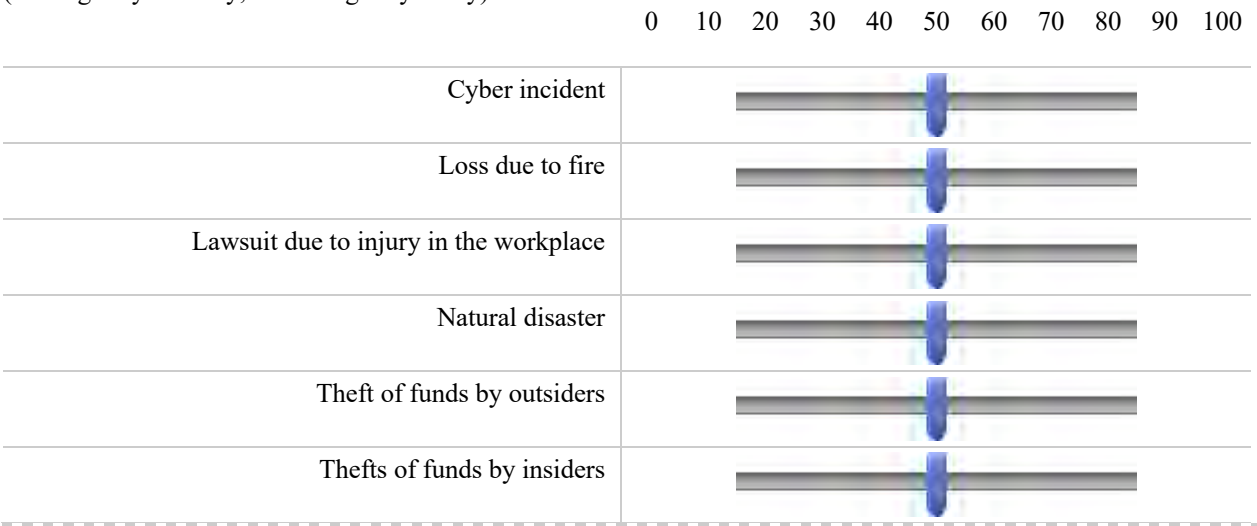
Q1.2 How concerned is your organization about the risk of a cyber incident?

- Not at all concerned
- Somewhat concerned
- Very concerned

Q1.3 Does your organization currently have an insurance policy that provides coverage for any of these events? (Select any that apply)

- Cyber incident
- Loss due to fire
- Lawsuit due to injury in the workplace
- Natural disaster
- Theft of funds by outsider
- Theft of funds by insider
- Not sure

Q1.4 How likely do you think it is that the following events will impact your organization? (0 being very unlikely, 100 being very likely)




*Carry Forward All Choices - Displayed & Hidden from "How likely do you think it is that the following events will impact your organization? (0 being very unlikely, 100 being very likely)"*

Q1.5 How much harm do you think your organization would face if each of the following events occurred? (0 being very little harm, 100 being a great deal of harm)

| | 0 10 20 30 40 50 60 70 80 90 100 |
|---|---|
| Cyber incident |  |
| Loss due to fire |  |
| Lawsuit due to injury in the workplace |  |
| Natural disaster |  |
| Theft of funds by outsiders |  |
| Thefts of funds by insiders |  |

Q1.6 What types of cyber incidents is your organization concerned about? (Select any that apply)

- Ransomware (e.g., extortion)
- Phishing (e.g., targeting key personnel through cyber-enabled means)
- Insider attack (e.g., an employee selling access or secrets)
- Malware (e.g., malicious software)
- Wire/financial fraud (e.g., theft of money through electronic means)
- Password attacks (e.g., someone else breaking your passwords)
- Denial of service attacks (e.g., someone making it impossible for users to access your website)
- Other (Please describe) _____

*Carry Forward Selected Choices from "What types of cyber incidents is your organization concerned about? (Select any that apply)"*

Q1.7 Please rank the potential types of cyber incidents you identified from most concerning to least concerning.

- Ransomware (e.g., extortion)
- Phishing (e.g., targeting key personnel through cyber-enabled means)
- Insider attack (e.g., an employee selling access or secrets)
- Malware (e.g., malicious software)
- Wire/financial fraud (e.g., theft of money through electronic means)
- Password attacks (e.g., someone else breaking your passwords)
- Denial of service attacks (e.g., someone making it impossible for users to access your website)
- Other (Please describe)

Q1.8 What potential consequences of cyber incidents is your organization concerned about? (Select all that apply)

- Data or information being exposed to outsiders
- Data or information being deleted or lost
- Disinformation about your organization being spread
- Identity theft
- Wire/financial fraud
- Website or system downtime
- Other (Please describe) _____

*Carry Forward Selected Choices from "What potential consequences of cyber incidents is your organization concerned about? (Select all that apply)"*

Q1.9 Please rank the potential consequences of cyber incidents you identified from most concerning to least concerning.

Data or information being exposed to outsiders
Data or information being deleted or lost
Disinformation about your organization being spread
Identity theft
Wire/financial fraud
Website or system downtime
Other (Please describe)

**End of Block: Cyber Risk Perceptions**

**Start of Block: Cyber Risk Management and Planning**

Q2.1 To your knowledge, has your organization experienced a successful cyber incident in the past three years?

Yes
No
Not sure or can't say

Q2.2 How many cyber incidents resulting in data theft did your organization experience in the last three years?

None
1-5
6-10
11-50
51-100
More than 100
Not sure or can't say

*Display This Question:*
*If How many cyber incidents resulting in data theft did your organization experience in the last thr... != None*
*And How many cyber incidents resulting in data theft did your organization experience in the last thr... != Not sure or can't say*

Q2.3 Please think back to the most severe cyber incident resulting in data theft experienced by your organization in the last three years. When did the cyber incident occur?

Month _____
Year _____

*Display This Question:*
*If How many cyber incidents resulting in data theft did your organization experience in the last thr... != None*
*And How many cyber incidents resulting in data theft did your organization experience in the last thr... != Not sure or can't say*

Q2.4 What type of cyber incident did your organization experience?

- Ransomware
- Phishing
- Insider attack
- Malware
- Password attacks
- Denial of service attacks
- Wire/financial fraud
- Other (Please describe) _____
- Not sure

*Display This Question:*
*If How many cyber incidents resulting in data theft did your organization experience in the last thr... != None*
*And How many cyber incidents resulting in data theft did your organization experience in the last thr... != Not sure or can't say*

Q2.5 What were the consequences of the cyber incident experienced by your organization?

- No consequences occurred
- Data or information being exposed to outsiders
- Data or information being deleted or lost
- Disinformation about your organization being spread
- Identity theft
- Wire/financial fraud
- Payment for credit monitoring services
- Website or system downtime
- Disruption of operations
- Other (Please describe) _____
- Not sure

Q2.6 Has your organization taken any steps to prevent potential cyber incidents?

- Yes
- No
- Not sure

*Display This Question:*
*If Has your organization taken any steps to prevent potential cyber incidents? = Yes*

Q2.7 What steps has your organization taken? (Select all that apply)

- Installed antivirus software
- Trained employees to spot potential cyber risks
- Invested in cyber risk insurance
- Limited physical access to computer systems
- Required employees to regularly change passwords
- Update and patch software regularly
- Other (Please describe) _____

*Display This Question:*
*If Has your organization taken any steps to prevent potential cyber incidents? = No*

Q2.8 Why hasn't your organization taken steps to prevent potential cyber incidents? (Select all that apply)

- Too expensive
- Too difficult
- Not sure what to do
- Prefer to spend resources on other priorities
- Options for preventing cyber incidents are ineffective
- Don't believe our organization is at risk
- Other (Please describe) _____
- Not sure

Q2.9 Has your organization taken any steps to mitigate potential cyber incidents?

- Yes
- No
- Not sure

*Display This Question:*
*If Has your organization taken any steps to mitigate potential cyber incidents? = Yes*

Q2.10 What steps has your organization taken? (Select all that apply)

- Installed automatic back-up systems
- Encrypted data
- Purchased cyber risk insurance
- Utilized cloud computing
- Other (Please describe) _____

*Display This Question:*
*If Has your organization taken any steps to mitigate potential cyber incidents? = No*

Q2.11 Why hasn't your organization taken steps to mitigate potential cyber incidents?

- Too expensive
- Too difficult
- Not sure what to do
- Prefer to spend resources on other priorities
- Don't believe our organization is at risk
- Other (Please describe) _____
- Not sure

Q2.12
Does your organization use any of the following tools to proactively manage the cyber threats facing your organization? (Select all that apply)

- Joined an information sharing group such as an ISAC
- Consulted news reports
- Relied on government data such as from IN-ISAC or US CERT
- Contacted the FBI/Secret Service for a briefing
- Revised and updated the organization’s incident response plan
- Launched a cyber hygiene campaign
- Revised organizational governance to ensure that cyber threat information was getting where it was needed.
- Other (Please describe) _____
- Not sure

Q2.13 Did your organization refer to any externally developed cyber tools, frameworks, or controls in making decisions about cyber practices?

- Yes
- No
- Not sure

*Skip To: Q2.15 If Did your organization refer to any externally developed cyber tools, frameworks, or controls in m... != Yes*

Q2.14 If so, which? (Select all that apply)

- NIST Cybersecurity Framework
- ISA
- ISME
- NISTIR 7621 Measure
- ISO 15408
- ISO 27001-02
- ETSI
- Center for Internet Security (CIS) Critical Security Controls
- SP 800-53 R4 Controls
- Australia Top 35 Controls
- Other (Please specify) _____

Q2.15 To your knowledge, has your organization provided anyone with training intended to raise awareness of the potential for cyber threats like hacking, phishing, spamming, or other threats related to stealing or compromising digital?

- Yes
- No
- Not sure

Q2.16 Did you receive training in a formal setting offered by your organization?

- Yes
- No
- Not Sure

*Skip To: Q2.18 If Did you receive training in a formal setting offered by your organization? != Yes*

Q2.17 How often have you attended trainings designed to improve your awareness of cyber threats?

- Once a quarter
- Once a year
- Every few years
- I have attended only one training

Q2.18 Have others in your organization received training in a formal setting offered by your organization?

- Yes
- No
- Not sure

Q2.19 Who in your organization is ultimately responsible for managing cyber risks?

- CEO
- Board of Directors Committee
- Chief Information Security Officers (CISO)
- Chief Information Officer (CIO)
- Chief Privacy Officer (CPO)
- Chief Information Governance Officer (CIGO)
- Other (Please specify) _____
- Not sure

Q2.20 How many cybersecurity professionals are currently employed at your organization?

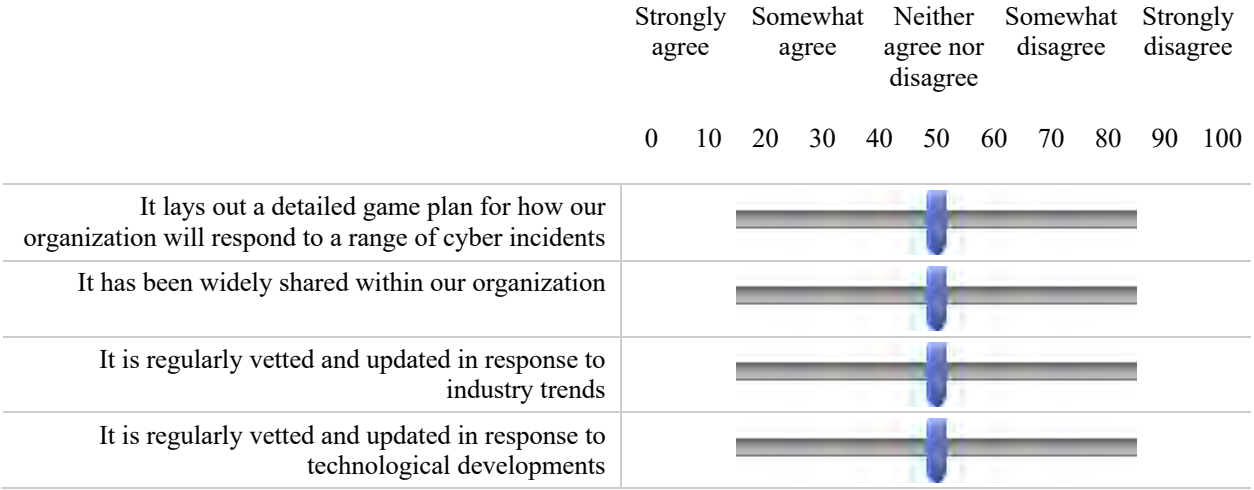
- None
- 1-5
- 6-10
- 11+

Q2.21 Does your organization have written documentation related to cyber incident planning and response?

- Yes
- No
- Not sure

*Skip To: Q2.23 If Does your organization have written documentation related to cyber incident planning and response? != Yes*

Q2.22 How strongly would you agree or disagree with the following statements about your organization's cybersecurity documentation?



Q2.23 Which, if any, of the following practices does your organization currently employ? (Select all that apply)

- Multi-factor authentication
- End-to-end encryption
- Remote backups
- Automatic updating of operating systems and software
- Traffic flow analysis
- Third-party penetration testing
- Policy on "Bring Your Own Device" (BYOD)
- Regular checks for vendors and partners
- Others (Please describe) _____
- None of the above
- Not sure or can't say

Q2.24 Does your organization currently have insurance specifically tailored to cover cyber incidents?

- Yes
- No
- Not sure

**End of Block: Cyber Risk Management and Planning**

**Start of Block: Cyber Risk Insurance Use**

Q3.1 When did your organization obtain a cyber risk insurance policy?

- Year _____
- Month _____

Q3.2 Why did your organization get a cyber risk insurance policy? (Select all that apply)

- Response to an incident at our organization
- Response to an incident at a peer organization
- News reports about cyber incidents
- Other (Please describe) _____
- Not sure

Q3.3 Which (if any) losses to your organization (first-party losses) are covered under this policy? (Select all that apply)

- Expenses related to responding to the cyber breach (such as hiring a firm to secure systems)
- Cost of notifying affected customers or others whose data was exposed in a breach
- Credit monitoring services
- Fines/penalties related to the data breach
- Business interruptions related to denial of service or other downtime
- Losses resulting from exposure or use of confidential business information
- Losses arising from stolen funds or products
- Damage to computer or information systems (including cost of restoring lost data)
- Damages related to lost intellectual property
- Forensic investigation of the breach
- Standing up a call center and response team
- Other (Please describe) _____
- None of the above
- Not sure

*Skip To: Q3.5 If Which (if any) losses to your organization (first-party losses) are covered under this policy? (S... = None of the above*
*Skip To: Q3.5 If Which (if any) losses to your organization (first-party losses) are covered under this policy? (S... = Not sure*

*Carry Forward Selected Choices from "Which (if any) losses to your organization (first-party losses) are covered under this policy? (Select all that apply)"*

Q3.4 Please rank how important it is for your organization to have coverage for the first-party losses you selected, from most important to least important.

Expenses related to responding to the cyber breach (such as hiring a firm to secure systems)
Cost of notifying affected customers or others whose data was exposed in a breach
Credit monitoring services
Fines/penalties related to the data breach
Business interruptions related to denial of service or other downtime
Losses resulting from exposure or use of confidential business information
Losses arising from stolen funds or products
Damage to computer or information systems (including cost of restoring lost data)
Damages related to lost intellectual property
Forensic investigation of the breach
Standing up a call center and response team
Other (Please describe)
None of the above
Not sure

Q3.5 Which (if any) losses to others (third-party losses) are covered under this policy? (Select all that apply)

Claims for damages from customers or others whose information was exposed in the breach
Claims for damages from customers or others who suffered other economic loss due to your security failure (e.g., malware was pushed to their systems)
Costs for legal defenses related to the data breach
Fines and penalties
Other (Please describe) _____
None of the above
Not sure

*Skip To: Q3.7 If Which (if any) losses to others (third-party losses) are covered under this policy? (Select all t... = None of the above*
*Skip To: Q3.7 If Which (if any) losses to others (third-party losses) are covered under this policy? (Select all t... = Not sure*

*Carry Forward Selected Choices from "Which (if any) losses to others (third-party losses) are covered under this policy? (Select all that apply)"*

Q3.6 Please rank how important it is for your organization to have coverage for the third-party losses you selected, from most important to least important.

Claims for damages from customers or others whose information was exposed in the breach
Claims for damages from customers or others who suffered other economic loss due to your security failure ( e.g., malware was pushed to their systems)
Costs for legal defenses related to the data breach
Fines and penalties
Other (Please describe)
None of the above
Not sure

Q3.7 Does your cyber risk insurance policy require your organization to undertake certain security measures?

Yes
No
Not sure

*Skip To: Q3.9 If Does your cyber risk insurance policy require your organization to undertake certain security mea... != Yes*

Q3.8 What security measures are required by your cyber risk insurance policy? (Select all that apply)

Mandatory, automatic patching
End-to-end data encryption
Employee training & cyber hygiene
Regular third party penetration testing
Other (please list) _____
None of the above
Not sure

Q3.9 Does your cyber risk insurance policy have a limit?

Yes
No
Not sure

*Skip To: Q3.11 If Does your cyber risk insurance policy have a limit? != Yes*

Q3.10 What is the limit?

_____

Q3.11 Does your cyber risk insurance policy exclude coverage in certain circumstances?

Yes
No
Not sure

*Skip To: Q3.13 If Does your cyber risk insurance policy exclude coverage in certain circumstances? != Yes*

Q3.12 Under what circumstances would your cyber risk insurance policy exclude coverage (Select all that apply)
- Act of war/terrorism
- Internet of Things-related breach
- Losses from unencrypted devices
- Contractual liability
- Criminal or fraudulent acts
- Losses related to unauthorized collection of customer data
- Losses that occurred because your organization failed to provide and maintain adequate security
- Other (Please describe) _____
- None of the above

Q3.13 Is your policy retroactive to cover losses that occurred (in whole or in part) before its start date?
- Yes
- No
- Not sure

Q3.14 Does your company require subcontractors to have cyber risk insurance?
- Yes
- No
- Not sure

*Skip To: End of Block If Does your company require subcontractors to have cyber risk insurance? != Yes*

Q3.15 What losses must be covered under a subcontractor's cyber risk insurance policy?
- Expenses related to responding to the cybersecurity breach (such as hiring a firm to secure systems)
- Cost of notifying affected customers or others whose data was exposed in a breach
- Fines/penalties related to the data breach
- Business interruptions related to denial of service or other downtime
- Losses resulting from exposure or use of confidential business information
- Not sure

**End of Block: Cyber Risk Insurance Use**

**Start of Block: Cyber Risk Insurance Non-Use**

Q4.1 Has your company ever had a cyber risk insurance policy?
- Yes
- No
- Not sure

*Skip To: Q4.6 If Has your company ever had a cyber risk insurance policy? != Yes*

Q4.2 During what period did your company have a cyber risk insurance policy?
- Date cyber risk insurance coverage began _____
- Date cyber risk insurance coverage ended _____

*Carry Forward All Choices - Displayed & Hidden from "Which (if any) losses to your organization (first-party losses) are covered under this policy? (Select all that apply)"*

Q4.3 Which (if any) losses to your organization (first-party losses) were covered under this policy? (Select all that apply)

- Expenses related to responding to the cyber breach (such as hiring a firm to secure systems)
- Cost of notifying affected customers or others whose data was exposed in a breach
- Credit monitoring services
- Fines/penalties related to the data breach
- Business interruptions related to denial of service or other downtime
- Losses resulting from exposure or use of confidential business information
- Losses arising from stolen funds or products
- Damage to computer or information systems (including cost of restoring lost data)
- Damages related to lost intellectual property
- Forensic investigation of the breach
- Standing up a call center and response team
- Other (Please describe) _____
- None of the above
- Not sure

*Carry Forward All Choices - Displayed & Hidden from "Which (if any) losses to others (third-party losses) are covered under this policy? (Select all that apply)"*

Q4.4 Which (if any) losses to others (third-party losses) were covered under this policy?

- Claims for damages from customers or others whose information was exposed in the breach
- Claims for damages from customers or others who suffered other economic loss due to your security failure (e.g., malware was pushed to their systems)
- Costs for legal defenses related to the data breach
- Fines and penalties
- Other (Please describe) _____
- None of the above
- Not sure

Q4.5 Why did you discontinue your former cyber risk insurance policy? (Select all that apply)

- Too expensive
- Couldn't get a policy
- Covered under other insurance policies
- Prefer to spend resources on other priorities
- Options for preventing cybersecurity incidents are ineffective
- Don't believe our organization is at risk
- Other (Please describe) _____
- Not sure

*Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Too expensive*
*Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Couldn't get a policy*
*Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Covered under other insurance policies*
*Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Prefer to spend resources on other priorities*
*Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Options for preventing cybersecurity incidents are ineffective*

*Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Don't believe our organization is at risk*
*Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Other (Please describe)*
*Skip To: Q4.6 If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Too expensive*
*Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Not sure*

Q4.6 Has your company ever considered obtaining a cyber risk insurance policy?
- Yes
- No
- Not sure

*Skip To: Q4.8 If Has your company ever considered obtaining a cyber risk insurance policy? != Yes*

Q4.7 Why did your company decide not to obtain a cyber risk insurance policy? (Select all that apply)
- Too expensive
- Difficult to obtain
- Covered under other insurance policies
- Prefer to spend resources on other priorities
- Options for preventing cybersecurity incidents are ineffective
- Don't believe our organization is at risk
- Other (Please describe) _____

Q4.8 What would encourage your company to obtain a cyber risk insurance policy?

_____
_____
_____
_____
_____

**End of Block: Cyber Risk Insurance Non-Use**

**Start of Block: Organization and Respondent**

Q5.1 What is your job title?

_____

Q5.2 How many employees does your organization have?
- 1-10 employees
- 11-50 employees
- 51-250 employees
- More than 250 employees

Q65 Does your organization fall within one of the following critical infrastructure sectors?

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector
- No, my organization does not fall within a critical infrastructure sector
- Prefer not to say

*Skip To: Q5.4 If Does your organization fall within one of the following critical infrastructure sectors? != No, my organization does not fall within a critical infrastructure sector*

Q5.3 What sector is your organization in?

- Accommodation and Food Services
- Administrative and Support Services
- Agriculture, Forestry, Fishing, and Hunting
- Arts, Entertainment, and Recreation
- Construction
- Educational Services
- Finance and Insurance
- Government
- Health Care and Social Assistance
- Manufacturing
- Mining
- Other Services
- Professional, Scientific, and Technical Services
- Real Estate, Rental, and Leasing
- Retail Trade
- Transportation and Warehousing
- Utilities
- Wholesale Trade
- Other (Please specify) _____

Q5.4 Which of the following types of information about individuals does your organization handle? (Select all that apply)

- Personally identifiable information (e.g., home addresses, email addresses, social security numbers)
- Personal financial information (e.g., credit card numbers, banking information, credit scores)
- Personal health information (e.g., allergies, past medications)
- Other (Please describe) _____
- We do not collect any personal data

Q5.5 How would you describe the geographic scope of your organization?

- Local (e.g., city or county)
- State
- Regional (e.g., more than one state)
- National
- Multi-national
- Does not apply

Q5.6 Would you be willing to participate in a follow-up interview to further explore how your company is managing cyber risk?

- Yes
- No

*Display This Question:*

*If Would you be willing to participate in a follow-up interview to further explore how your company... = Yes*

Q5.7 Thank you for your willingness to participate in a follow up interview. Please provide your name, affiliation, and email for contact purposes only.

_____

**End of Block: Organization and Respondent**


# Appendix D.14
## Privacy Working Group

# PRIVACY WORKING GROUP STRATEGIC PLAN

Chair: Tracy Barnes
Co-Chair: Leon Ravenna


October 2021
Indiana Executive Council on Cybersecurity

# Privacy Working Group Plan

# Table of Contents

# Committee Members

# Committee Members

| Last Name | First Name | Organization | Organizational Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Babione | John | Dinsmore & Shohl LLP | Partner | Full Time |
| Barnes | Tracy | Indiana Office of Technology | Chief Information Officer | Chair |
| Berry-Tayman | Lisa | Kevel | Director of Security and Privacy | Full Time |
| Braidich | Richard | RCR Technology | Chief Information Security & Privacy Officer | Full Time |
| Britt | Luke | Indiana Office of Public Counselors | Public Access Counselor | Full Time |
| Dimon | Philip | Indiana Department of Revenue | Information Security Manager | As Needed |
| Donahue | Matthew | Consultant | Consultant | Full Time |
| Heir | Rajinder | Indiana Commission for Higher Education | Chief Technology Officer | Full Time |
| Lacy | Peter | Indiana Bureau of Motor Vehicles | Commissioner | As Needed |
| Mabry | Kevin | Sentree Systems Corp. | CEO/President | As Needed |
| McCullough | Cliff | Family and Social Services Administration | Chief Privacy Officer | Full Time |
| Prostko | Robert | Allegion, plc | Deputy General Counsel, Cybersecurity and Intellectual Property, and Chief Privacy Officer and Principal at Allegion Ventures | Full Time |

| | | | | |
|---|---|---|---|---|
| Ravenna | Leon | KAR Global | Chief Information Security Officer | Co-Chair |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

# 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 Templates
    - https://www.in.gov/idoa/files/2021-Professional-Services-Contract-Template.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 Privacy Framework, Version 1.0
    - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf
    - NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*
    - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.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-17-12, *Preparing for and Responding to the Breach of Personally Identifiable Information*
    - https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.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
  - FTC Report, Resources Used and Needed for Protecting Consumer Privacy and Security

        - https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf
    - IAPP Glossary of Privacy Terms
        - https://iapp.org/resources/glossary/
    - SANS CIS Critical Security Controls
      https://sansorg.egnyte.com/dl/DxG01UgWeQ

- **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 that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.."[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-17-12.
[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.

- **2021 Working Group Deliverables**
    - PII Guidebook 2.0
    - Indiana Privacy Toolkit

- **Additional Notes**
    - All referenced Research Conducted is available via the embedded link or as an attachment to this document.

# Research

# Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** There are several initiatives that IOT has led or been very involved with since 2015 around the topic of cybersecurity.
  - Indiana established a central information technology office in 2005 under an executive order by former Gov. Mitch Daniels and codified by the legislature that same year. Security was a focus from day one. The Office of Technology (IOT) has been tasked with reviewing, among other things, projects architecture and security. The state appointed its first chief information security officer (CISO) shortly after creating IOT.
  - The State initially focused on protecting agency applications, websites and developed policies and standardized fundamental security practices such as end-point protection, network segmentation, penetration process and risk assessments.
  - IOT, Purdue University, Cisco, FireEye & RSA partnered to create the Indiana Information Sharing & Analysis Center (IN-ISAC) in 2015. The IN-ISAC provides real-time network monitoring, vulnerability identification and threat warnings.
  - In 2016, the State of Indiana organized and participated in a critical infrastructure readiness and resiliency exercise utilizing an Indiana National Guard facility. The simulated cyberattack used a utility SCADA system housed on a separate grid, which allowed real attacks and results to occur. A variety of utility personnel manned the SCADA system while attacks occurred to see how they would respond.
  - Indiana expanded its cybersecurity program through Executive Order 17-11, signed by Gov. Eric Holcomb in 2017. It is recognized nationally and led by the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana State Police, and the Indiana National Guard and the Indiana Executive Council on Cybersecurity (IECC). Recognized for its unique structure, the membership of the Council is comprised of government officials (local, state, and federal), as well as stakeholders and experts from the private-sector, military, research, and the academic community.
  - Indiana's cybersecurity program is centered on proactively providing guidance and resources to all Hoosiers, including units of local governments, businesses across a wide range of industries and markets, as well as to our K-12 schools, colleges, and universities.

- **INDIANA COMMISSION FOR HIGHER EDUCATION (CHE)**: Speaking only for CHE in all responses, CHE emphasizes awareness with staff at every reasonable opportunity to do so in a constructive fashion. In all of 2020 and 2021 Q1 and Q2, CHE staff achieved 100% each quarter on the KPI for completion of cyber sec awareness training. We have previously signed up for extra phishing tests w/IOT. CHE implemented an app sec platform in 2020. Implemented two-factor for a mission critical application. More broadly, we prepared a report in 2020 on cyber sec talent pipeline from higher ed perspective.

- **ALLEGION**:
  - Board and executive level training
  - Technologist training
  - Global employee training
  - Industry speaking engagements
  - Several employees have pursued undergraduate and graduate degrees as well as industry certifications in cybersecurity
  - Leveraged outside experts for specific types of training
  - Subscribe to services for security awareness training
  - Self-study webinars and phishing events
  - Conduct cyber ranges open to all employees

- **SENTREE SYSTEMS:** Being a part of the community and offering training and educational speaking engagements to help businesses to understand the threat landscape.

- **KAR GLOBAL:**
  - Moved from a monolithic once per year training to more frequent (every other month) shorter training vignettes. Stringing together 4-5 60-90 second vignettes together every other month with a testing component once a year. Delivering shorter training more frequently increased awareness.
  - Performing frequent (quarterly) phish testing
  - Ad hoc training emails, intranet articles and reminders going to all employees, with at least 1 per month for a constant reminder.
  - Routine tabletop exercises
  - Multiple events/ articles for Cybersecurity Awareness month, Data Privacy Day

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

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** Employees and contractors, the human element, remain the greatest vulnerability to the State of Indiana. The number one weakness is staff clicking on a link opening an attachment or inadvertently releasing credentials that allow an attacker an entry vector.

- **CHE:** System vulnerabilities. Staff awareness – sustaining a high level of cyber awareness among CHE employees. We have significant volume of PII we must protect.

- **ALLEGION:** No Response

- **SENTREE SYSTEMS:** Ransomware, and email scams are the most significant attack vectors in my industry.

- **KAR GLOBAL:** Similar to most organizations email is the number one threat vector and the preferred delivery vehicle for ransomware.

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

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** The State of Indiana has a robust cybersecurity training program required of all employees and contractors. This monthly training is built on a variety of learning materials and builds upon each other, as well as reviews concepts. Despite the success of this program, cybersecurity defense requires 100% success. Any mistake or erroneous click can open the network allowing an attacker to slip in.

- **CHE:** Resources (human + financial) to sustain and mature a cyber sec program. This includes robust level of protection of the information entrusted to us, continuous work on cyber awareness, routine app sec assessment, maintaining skilled staff. Users expect a frictionless experience and cyber sec measures are not always conducive to such (i.e., least privilege, two factor, passphrases).

- **ALLEGION:** Sustained investment and keeping pace with modernization

- **SENTREE SYSTEMS:** The biggest gap observed is in the small business area in the detection and response layer of security. The protection layer is robust, but there is nothing to cover these small businesses if and when an attack happens.

- **KAR GLOBAL – answering in general observation on the state of companies:**
  - Gaps for most companies continue to be training and general cybersecurity hygiene.
  - For global companies, the inability to think beyond the shores of US or North America is a large gap. Particularly, when networks are connected. Forgetting about the groups outside North America is to their detriment.
  - Inability to roll out and sustain security product effectiveness. Basically, buy a product but not fully exploit its capabilities or features.
  - Inability to understand where the threats come from (APIs, exposed S3 buckets, inability to secure cloud. Particularly, those lift & shift applications.

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

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** The State of Indiana must follow federal compliance laws in cybersecurity, especially in areas of health and human services and taxes. The State has developed cybersecurity regulations that are created and managed by the Indiana Office of Technology. These policies are applicable to all state agencies.

- **CHE:** FERPA and applicable state level regulations and policies apply to CHE.

- **ALLEGION:**
  - GDPR
  - CCPA
  - HIPAA
  - Australia's Privacy law
  - China's Privacy law

- **SENTREE SYSTEMS:** Based on review, only state PII regulations apply to Sentree.

- **KAR GLOBAL:**
  - GDPR, CCPA
  - Customer demands across multiple industries

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** The Indiana Office of Technology's security department is glad to have discussions about its programs and services.

- **CHE:** Cannot answer adequately at this time.

- **ALLEGION:** N/A

- **SENTREE SYSTEMS:** N/A

- **KAR GLOBAL:** N/A

6. **What research is out there to validate your group's preliminary deliverables?**

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** Not applicable

- **CHE:** Cannot answer adequately at this time.

- **ALLEGION:**
  - https://owasp.org/www-project-top-ten/
  - https://www.verizon.com/business/solutions/secure-your-business/business-security-tips/#dbir
  - https://www.ponemon.org/research/ponemon-library/

- **SENTREE SYSTEMS:** No Response

- **KAR GLOBAL: N/A**

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**

   - **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** Other States are also investing in employee and contractor training around cybersecurity, promoting a culture around shared responsibility and risk mitigation helps drive towards desired behavior. Phishing simulations, tabletop exercises are two examples of educating and preparing for an attack.

   - **CHE:** I expect peers are doing their part. Rather than pasting a random link from a quick search, I am not sufficiently knowledgeable on a specific state's effort. In 2020 CHE published a report on the cyber sec higher education pipeline and we will update this report in 2022.

   - **ALLEGION:** No Response

   - **SENTREE SYSTEMS:** There are a few, but not many offering a more continuous cyber training service to their employees and clients. It is the opinion of this committee that continuous cyber training is superior to free training or a one-year training offering.

   - **KAR GLOBAL:** N/A

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

   - **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** Cybersecurity success is not a one and done event. There is no checking of the box to indicate we are done. This is an ongoing effort to continue to implement best in class support around our people, process and technology. Metrics can help drive towards increased adoption of cybersecurity policies, better phishing simulation results, and increased business enablement while operating within our risk appetite.

- **CHE:**
  - One year – establish a security program (to include a charter, routine app sec assessments, cyber sec awareness training goals, policy dev). Measure against a maturity model.
  - Three years – (with adequate resources) sustained progression on maturity model scale. Social Sec Admin comes up w/better alternative to SSNs. No breaches.
  - Five years – continued funding/resources to match the need. Accountability - prosecution of those behind every cyberattack.

- **ALLEGION:** No Response

- **SENTREE SYSTEMS:**
  - Year 1 – expand on the education of MSP's that they need help from security experts.
  - Year 2 – build out a more aggressive approach to cyber threats and utilize the knowledge from cyber experts
  - Year 3 – MSP's build in security in their offerings, not just another line item, it needs to be built-in
  - Year 5 – Have a more streamline approach between MSP's and cyber security experts

- **KAR GLOBAL:**
  - Key success over any timeframe is not being breached.
  - Over the next year,
    - Drive application changes further left in the development cycle to lower the cost of fixing flaws that may be found in applications.
    - Integrate global support services while maintain data sovereignty for Privacy frameworks such as GDPR.
  - Over the course of the next 3 years,
    - Drive deeper security controls into public cloud environments.
    - Retain key skill sets
    - Devise consistent patterns for hiring those with raw skills that can be developed.
  - Within 5 years, build cybersecurity awareness into the DNA of the organization

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

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** The State of Indiana already has a robust training program for state employees and contractors.

- **CHE:** Inform (not scare) audiences, using VOC-style (voice of the customer) communication. Meet target audiences where they are. Leaders of nonprofits, and small business owners can easily be overwhelmed by all they are to protect, and how to do it with layman-level knowledge. Tap into local chambers of commerce to share info/programs w/small biz.

- **ALLEGION:** No Response

- **SENTREE SYSTEMS:** Offer free trainings, although participation may be low if they are free and there is no mandate on them. More training initiated and facilitated through employers to their employees would be more effective. Training does not stop at the employer's door. It is best when the employees take the same knowledge home and can utilize it in their personal lives.

- **KAR GLOBAL:** 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?**

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** The Office of Technology has approximately 500 staff members, including around 30 that work specifically in security.

- **CHE:** CHE is a state agency with no dedicated cyber security resources on staff. It would be desirable to have .5 FTE dedicated to establishing all facets of a security program to begin with.

- **ALLEGION:** No Response

- **SENTREE SYSTEMS:** One person

- **KAR GLOBAL:** N/A

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

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** Not applicable to IOT.

- **CHE:**
    - Improve quality of life indicators (i.e. smoking, obesity, infant mortality, high school graduation rates, etc.)
    - Build the new graduate talent (while attracting businesses) to create success stories
    - Secure partnerships with the private sector (i.e. Honda) to encourage new cybersecurity graduates to stay in Indiana by establishing a program that offers a free car for 5 years post-graduation

- Encourage start-up/participation in a professional network, meet a significant other, purchase a home or establish a cybersecurity startup business (possible role for TechPoint)
- Necessity for competing with higher salaried jobs (compared to other areas), with the offer of a car as an incentive for cybersecurity graduates.

- **ALLEGION:** No Response

- **SENTREE SYSTEMS:** An educated environment of businesses and MSP's willing to work together and share knowledge would help.

- **KAR GLOBAL:**
  - To attract cyber companies is a public/ private sector issue. Seeing high tech companies such as Exact Target and Interactive Intelligence start and be sold in Indiana provides the proof that it can be done. The combination of high-tech companies, low cost of living, talent pipelines from Purdue, Rose Holman, and state incentives will surely help as many companies look to relocate to low cost/ tax environments.

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

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** The State of Indiana has developed an Incident Response Plan and offers additional resources to assess cybersecurity preparedness, including the Indiana Cybersecurity Scorecard. Developed by the State of Indiana and Purdue University, this 22-question tool will provide a score of where an organization stands in cybersecurity with easy-to-understand questions.

- **CHE:** While we would work in conjunction with IOT, this is an area we need to shore up internally.

- **ALLEGION:** Companies should align to an industry standard such as ISO/IEC 27035-1:2016

- **SENTREE SYSTEMS:** No Response

- **KAR GLOBAL:**
  - KAR utilizes a SIRT (Security Incident Response Team) for any issues. This team has the authority to stop processes and bring in any resources at a moment's notice if there is an issue found.
  - The Incident Response Plan has built-in communications plans for business resources, outside law enforcement and media.

**13. What best practices should be used across the sectors in Indiana?**

- **STATE OF INDIANA OFFICE OF TECHNOLOGY (IOT):** The state requires each of its vendors to follow best practices and strict guidelines. Indiana's cybersecurity strategy relies on a common-sense approach and encourages those entities who partner with us to utilize the best practices and industry standards, as defined by NIST and other accepted guidance as provided by USDHS, CISA and FEMA, among others.

  The cybersecurity posture for the State of Indiana is supported by several principles outlined by Governor Holcomb through the Executive Order 17-11 and proclamation Gov. Holcomb issues the State of Indiana observes October as Cybersecurity Awareness Month.

- **CHE:** Best practice – establish a security program, assess/benchmark a score and routinely measure against a maturity model. Communicate the score to decision-makers. This applies to organizations of all sizes, regardless of sector. Convene thought-leaders across sectors for collaborative opportunities.

- **ALLEGION:** Government agencies and companies should align to or be certified to industry standards such as ISO 27001 or NIST 800

- **SENTREE SYSTEMS:** No Response

- **KAR GLOBAL:**
  - The nest frontier in cyber is fully understanding the whole supply chain. Including 3rd, 4th and 5th party suppliers. This includes having provision built in to react quickly when supply chain issues (SolarWinds, Kaseya, CodeCov) are found.

# Deliverable: Indiana PII Guidebook 2.0

# Deliverable: Indiana PII Guidebook 2.0

## *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

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?**
   ☐ 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. Pragmatic and useful definition for ease of application by end users.
   b. Generation of a highly useful 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?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. This resource is unique in that it captures the big-picture of federal guidance, and the local picture of Indiana-specific legal and practical guidance.

## 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. Privacy 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 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?**

☒ One-time deliverable
☐ Ongoing/sustained effort

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Review PII Guidebook | Privacy Working Group | 75 | Jan 2022 | |
| Characterize the current state | Privacy Working Group | 75 | Jan 2022 | |
| Identify additional regulations that should be included | Privacy Working Group | 75 | Jan 2022 | |
| Identify additional best practices across all sectors | Privacy Working Group | 75 | Jan 2022 | |
| Send to Privacy Team to review and make edits | Privacy Working Group | 0 | Feb 2022 | |
| Vote on final by the Privacy Team | Privacy Working Group | 0 | April 2022 | |
| Distribute to IECC, post online, and find other places where it should be referenced | Cyber Program Director | 0 | April 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

**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?**

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

**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 updated 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. No Response

**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 non-profit, and local government 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?**

☐No ☒ Yes

a. All sectors

## 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)?**

☐No ☒ 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 Privacy Working Group will update the Indiana PII Guidebook for government and general public by the end of April 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: Indiana Privacy Toolkit

# Deliverable: Indiana Privacy Toolkit

## *General Information*

1. What is the deliverable?
   a. Indiana Privacy Toolkit.
      i. To be written in a "voice of the Customer" style (e.g., FAQ)
      ii. Readers to gain:
         1. Basic understanding of PII
         2. Understand categories of PII that must be protected
         3. Starter knowledge of which regulations may apply to their organization
         4. Tips on how to establish a data privacy program
         5. Actionable list of best practices (p.14 from Guidebook)
         6. Turnkey policy templates (re-purposed from Guidebook plus additions)

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?**
   ☐ 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. For users (especially small business, nonprofits, and local governments) to use the Toolkit to gain increased awareness of PII, and applicable regulations. Take action to implement at least three foundational policies.

6. **What metric or measurement will be used to define success?**
   a. Completion of the deliverable. Site tracking to quantify views of Toolkit and downloads of specific policy templates.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Any user can benefit from this deliverable, but this is especially true for small business, nonprofits, and local governments.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. All state agencies on the IECC and State Privacy Officer will determine if there are programs that overlap with deliverable. All federal partners with the IECC will determine if there are programs that overlap with the deliverable.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Consult other industries and critical infrastructure committees for privacy best practices and policy templates applicable for the Toolkit's target audiences

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. All state agencies on the IECC and State Privacy Officer will determine if there are programs that overlap with the deliverable. All federal partners with the IECC will determine if there are programs that overlap with the deliverable. Nonprofit aggregators (such as associations of multiple nonprofits) can play a role in amplifying the deliverable to their groups.

12. **Who should be main lead of this deliverable?**
    a. State of Indiana CIO (chair of Privacy Working Group) co-leading with the CHE CTO (who is a member of the Privacy Committee).

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

a. Primarily time of the IECC members to complete the deliverable, especially given the limitations of COVID-19 on member's workload and availability to collaborate. Secondly, compiling all content in the Toolkit in a Voice of the Customer style (e.g. FAQ) to stay true to the concept behind the idea.

## *Implementation Plan*

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

☐ One-time deliverable

☒ Ongoing/sustained effort

### Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Developing an outline draft of the toolkit | Rajinder | 25 | March 2022 | |
| Break out sections of the PII Guidebook to be reused in the toolkit (see notes below) | Working Group Members | 10 | March 2022 | |
| Determine other polices to add to the toolkit (see notes below) | Working Group Members | 25 | March 2022 | |
| Develop site map for online toolkit | IECC Program Communications Manager | 0 | April 2022 | |
| Draft sections of toolkit | Working Group Members | 0 | May 2022 | |
| Edit sections of toolkit | Working Group Members and IOT support | 0 | June 2022 | |
| Finalize toolkit | Working Group Members and IOT support | 0 | June 2022 | |
| Go live with Privacy toolkit | State of Indiana | 0 | July 2022 | |
| Develop PR Launch Plan | IECC Program Communications Manager | 0 | June 2022 | |
| Implement PR Launch Plan | IECC Program Communications Manager and partners | 0 | July 2022 | |
| Measure views & downloads | IECC Program Communications Manager | 0 | December 2022 | |
| Update Toolkit | Working Group Members | 0 | Annually | |

*Notes for draft outline of Toolkit (cross references Guidebook content):*

- Page 1 - Intro section - add mention of very small business example and small nonprofit. Add - Who Should Read This and Why?
- Page 3 - What is PII?
- Page 6 – What MUST I read? PII categories that must be protected – showcase this table. If you only read the basics – this is critical content.
- Page 8 – What is the current state of PII? – should this be updated at specific intervals? Annually or more frequently? Or leave this in Guidebook and link to it?
- Page 10 – privacy regs – make this a table by sector or vertical market. Cheat sheet style?
- Page 12 – future dev – same as for page 8. Good info here.
- Page 14 – best practice. VOC style – What should my organization be doing? Checklist w/action words. i.e. #2 'Make your customers aware of cyber concerns'. Showcase this section. Add – a new first item - Establish a Privacy Charter and Committee or at minimum a point-person to lead? How to setup a (cyber/privacy) policy framework? Should this be addressed in this guidebook?
- Existing policy templates – add constituent or client (some nonprofits, such as shelters, may call the individuals they serve clients not customers).
- How do I establish a data privacy program?
- Appendices
  - Internal Privacy Policy – section 2 – scope, second para "regardless of where' – 'regardless of where or what medium' – to include paper?
  - IT Policy – could also be called Acceptable Use
- Other privacy related policy templates to consider for Toolkit:
  - Data Classification Standard (or tool template)
  - Destruction and disposal of storage media (for IT)
  - Business Use of Personal Mobile Devices
  - Employee Responsibility to Mitigate Cyber Risk – probable overlap w/IT Policy already in Guidebook
  - Data Retention

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1 | No Response | Technical Writer/Editor to ensure ease of readability | State of Indiana | Grants | |
| 1 | No Response | Communication Manger to assist in laying it out online and track progress | State of Indiana | Grants | |

**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 |
|---|---|---|---|---|---|---|
| No Response | | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Increased cyber security and data privacy awareness among small entities across sectors. At minimum readership of the Toolkit can be measured by views and downloads of each policy template.

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

a. It will meet audiences where they are in order to increase the likelihood, they will take basic actions (e.g., implement 3 key policies) to protect the data they are entrusted with. Cost of reduction in risk is largely reflective of the time of IECC members to compile to the Toolkit.

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

a. It leaves leaders of small entities across sectors to seek actionable information from many other sources which can be overwhelming.

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

a. First success definition is to complete and go live with the toolkit online. Second success definition is to determine a goal of users who have viewed the toolkit and downloaded parts of it to use by a certain timeframe.

**21. 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. Private associations and federal programs have components of toolkits that will be looked at and used on this toolkit.

**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?**

☒No ☐ Yes

## Other Implementation Factors

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

a. Personnel resources, major change in laws that affect the content of the toolkit.

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

☒No ☐ Yes

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

a. It will take members of the council and respective state agencies and other IECC committees to keep the content of the toolkit accurate and up to date.

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

a. Secondary research was conducted online. But working with the IECC Legal and Insurance Working Group to assist in keeping some parts of the toolkit up to date.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes,

a. All sectors can use this if they have data

## Communications

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

a. All organizations, especially non-profits, local governments, and small businesses.

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

☐No ☒ Yes

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

a. A full public relations campaign should be developed with the assistance of the IECC Cyber Awareness and Sharing Working Group and IECC Communication Program Manager.

## *Evaluation Methodology*

**Objective 1:** IECC Privacy Working Group develop an Indiana Privacy Toolkit for the Indiana business community, public sector, and local government by July 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

**Objective 2:** At least 200 users have accessed/downloaded the Indiana Privacy Toolkit for the Indiana business community, public sector, and local government by April 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

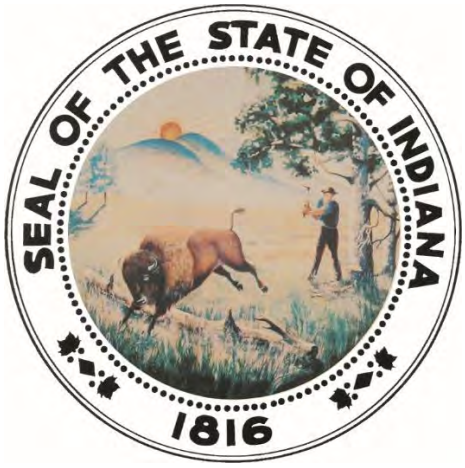
# Supporting Documentation

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

- State of Indiana PII Guidebook v. 1

# State of Indiana PII Guidebook v. 1

# Personally Identifiable Information (PII) Guidebook




**Personally Identifiable Information Working Group of the Indiana Executive Council on Cybersecurity**

**January, 2021**

**TABLE OF CONTENTS**

## INTRODUCTION TO THE PII GUIDEBOOK

Formed by the Indiana Executive Council on Cybersecurity, the Personally Identifiable Information Working Group (the "PII Working Group") is made up of private and public sector leaders in Indiana's privacy and cybersecurity realms. The PII Working Group has been tasked with the following:

- defining and characterizing the PII realm;
- identifying related regulations;
- addressing potential future developments; and
- identifying best practices and providing sample policies that can be implemented by businesses in any sector with the aim of mitigating cyber threats while enhancing the privacy, security, accuracy, availability, and integrity of digital information.

This guidebook can be leveraged by Indiana businesses, small and large, to identify the information that requires a heightened degree of protection. Whether your role is to collect basic customer information at the service counter at your business in Columbia City, validating information in cargo containers at the Port of Indiana-Mount Vernon, or processing medical claims in Indianapolis, the collection and maintenance of PII in your systems adds risk to your operation. This risk can be realized by the inadvertent disclosure of PII, which can cause harm in operational, legal, and reputational contexts. These risks can be mitigated by collecting only that PII which is required to complete a given transaction. To do that, we must understand what constitutes PII in our daily lives. This guidebook intends to help you gain that understanding.

**ACKNOWLEDGEMENTS**

A special thank you to members of Indiana Executive Council on Cybersecurity's PII Working Group who stepped forward to offer their expertise through this document. Specific mention is warranted for John Babione, Richard Braidich, Dom Caristi, Tony Chu, Ted Cotterill, Dewand Neely, Mitch Parker, Leon Ravenna, and Ashley Schenck. Additionally, thank you to Indiana Cybersecurity Program Director Chetrice Mosely for her support throughout the drafting and review process and to members of the Indiana Executive Council on Cybersecurity for their guidance. Lastly, thank you to Governor Eric Holcomb for his leadership, without which, the State of Indiana would not be leading the charge in cyber readiness.

## DEFINING PERSONALLY IDENTIFIABLE INFORMATION ("PII")

*PII Guidance Sources*

The purpose of this section is to identify and evaluate several definitions of PII to determine the specific data elements that should be regarded and protected as PII.

- Centers for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Department of Homeland Security (DHS) Handbook for Safeguarding Sensitive Personally Identifiable Information, March 2012
- Health Insurance Portability and Accountability Act (HIPAA)
- Indiana Code (IC) 4-1-6, Fair Information Practices; Privacy of Personal Information
- IC 4-1-11-3, Notice of Security Breach; Personal Information
- IC 35-43-5-1(i), Forgery, Fraud, and Other Deceptions; Identifying Information
- Internal Revenue Service (IRS) Publication 1075
- National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53
- Office of Management and Budget (OMB) Memorandum 06-19
- OMB Memorandum 07-16

*PII Guidance Sources and Definitions*

| SOURCE | DEFINTION |
|---|---|
| CMS MARS-E | As defined by National Institute of Standards and Technology (NIST) Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." |
| DHS | Some categories of PII are sensitive as stand-alone data elements. Examples include: SSN, driver's license or state identification number, passport number, alien registration number, or financial account number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII. |
| HIPAA | Pursuant to NIST Special Publication 800-66, Rev 1, "Individually Identifiable Health Information (IIHI) [45 C.F.R. Sec. 160.103], Information that is a subset of health information, including demographic information collected from an individual, and:<br>(1) Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and<br>(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and<br>(i) That identifies the individual; or<br>(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.<br><br>Protected Health Information (PHI) is a form of PII. It is IIHI that is:<br>• Transmitted by electronic media;<br>• Maintained in electronic media; or |

| | |
|---|---|
| | • Transmitted or maintained in any other form or medium.<br><br>PHI excludes IIHI in:<br>• Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;<br>• Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and<br>• Employment records held by a covered entity in its role as employer. |
| IC 4-1-6 Indiana Fair Information Practices Act | “Personal information" means any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual including, but not limited to, the individual's education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs, or the individual's presence, registration, or membership in an organization or activity or admission to an institution. |
| IC 4-1-11-3 Notice of Security Breach (as applicable to State agencies) | "Personal information" means:<br>(1) an individual's:<br>(A) first name and last name; or<br>(B) first initial and last name; and<br>(2) at least one (1) of the following data elements:<br>(A) Social Security number.<br>(B) Driver's license number or identification card number.<br>(C) Account number, credit card number, debit card number, security code, access code, or password of an individual's financial account. |
| IC 35-43-5-1(i) Identifying Information (as applicable to forgery, fraud, and other deceptions) | "Identifying information" means information that identifies a person, including a person's:<br>(1) name, address, date of birth, place of employment, employer identification number, mother's maiden name, social security number, or any identification number issued by a governmental entity;<br>(2) unique biometric data, including the person's fingerprint, voice print, or retina or iris image;<br>(3) unique electronic identification number, address, or routing code;<br>(4) telecommunication identifying information; or<br>(5) telecommunication access device, including a card, a plate, a code, a telephone number, an account number, a personal identification number, an electronic serial number, a mobile identification number, or another telecommunications service or device or means of account access that may be used to:<br>(A) obtain money, goods, services, or any other thing of value; or<br>(B) initiate a transfer of funds. |
| IRS PUB 1075 | Federal Tax Information (FTI) may include Personally Identifiable Information (PII). FTI may include the following PII elements:<br>• Name of a person with respect to whom a return is filed<br>• Taxpayer mailing address<br>• Taxpayer identification number<br>• E-mail addresses<br>• Telephone numbers<br>• Social Security Numbers<br>• Bank account numbers<br>• Date and place of birth<br>• Mother’s maiden name<br>• Biometric data (e.g., height, weight, eye color, fingerprints)<br>• Any combination of the above |

| | |
|---|---|
| NIST SP 800-122 | PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Examples of PII include, but are not limited to:<br>• Name, such as full name, maiden name, mother's maiden name, or alias<br>• Personal identification number, such as social security number, passport number, driver's license number, taxpayer identification number, or financial account or credit card number<br>• Address information, such as street address or email address<br>• Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)<br>• Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information) |
| OMB Memorandum 06-19 | Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. |
| OMB Memorandum 07-16 | 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. |

*Observations and Analysis*

The above list of PII definitions is not an exhaustive one, but they reasonably represent all relevant definitions for the purpose of this guidebook. Almost all of the examined definitions start with a general description that PII is any information that can be used to distinguish or trace an individual's identity, followed by examples of PII. No source provides a comprehensive list of PII data elements.

The DHS definition specifies the difference between two different types of sensitive PII—stand-alone and if paired with another identifier. DHS gives examples of stand-alone sensitive PII as social security, driver's license, and alien registration numbers. Alone, this data can be used to access a great deal of personal information. In contrast, DHS explains that other information, like medical information, date of birth, and mother's maiden name is not sensitive PII unless combined with other identifying information like the name of the individual to which it relates.

Based on the DHS guidance, the next section of this guidebook defines data elements that are Singularly PII and Collectively PII. Singularly PII data elements will be consistent with the DHS definition of stand-alone sensitive PII. Collectively PII data elements will be consistent with the DHS definition of PII that is sensitive when paired with another identifier.

While not identified in any of the above definitions, organization-specific data can also be PII. To illustrate, a unique identification number associated with a customer's record containing sensitive information in an organization's system could be considered PII if the name of the system were known. In another case, an

organization's record of answers to normally non-sensitive questions might be PII if they are answers to challenge questions when a user attempts to log into the organization's system without their password. Consequently, the next section of this guidebook also identifies examples of organization-specific PII.

*Summary of Categories of PII That Must Be Protected*

| Singularly PII | Collectively PII | Organization-specific PII |
|---|---|---|
| **Any of the following single items:**<br>• Social security number<br>• Alien registration/green card number<br>• State identification number<br>• Driver's license number<br>• Passport number<br>• Full credit card number<br>• Full financial account number | **Contains individual's name to include full first and last name or first initial and full last name, and at least one of the following:**<br>• Mother's maiden name<br>• Date of birth<br>• Place of birth<br>• Address (street or PO Box)<br>• Email address<br>• Phone number<br>• Employer or business name<br>• Citizenship or immigration status<br>• Ethnic affiliation<br>• Religious affiliation<br>• Sexual orientation<br>• Lifestyle preferences<br>• Employment history<br>• Wage history<br>• Financial transactions<br>• Customer amount owed, received, paid, collected, withheld, intercepted, earned, fined, and garnished<br>• The following types of information and records<br>- Medical<br>- Biometric<br>- Education<br>- Financial<br>- Tax<br>- Criminal/incarceration<br>- Social welfare | **Includes:**<br>• Login ID and password to organizational network, computing equipment, or applications hosting customer or employee data<br>• Account numbers associated with sensitive customer or employee records<br>• Customer or employee challenge questions and answers<br>• Employee performance records |

Most government agency definitions of PII are not specific enough to enable those responsible for protecting it to fully understand what data they are trying to protect. Part of that challenge relates to the evolving definition of PII, which is addressed in more detail later in this guidebook. To assist those wrestling with these issues, this guidebook provided (above) as comprehensive of a list of specific PII data elements as can be provided.

The table above and the other information provided in this guidebook should enable individuals, small business owners, and large industry and government organizations, who have an interest in or legal obligations to protect PII, to be more effective. It is important to understand, however, that the definition

of PII varies for different states within the Unites States and varies across the globe by nation. Accordingly, for organizations operating in multiple states and/or internationally, the definition and regulation of PII in those other jurisdictions should be carefully reviewed.

## CHARACTERIZING THE CURRENT STATE OF PII

Companies, consumers, and governments alike should be prepared for ever-evolving definitions and regulations surrounding the handling and security of PII, particularly in the near-term. The development and adoption of new technologies has grown rapidly in the 21st century. Enhanced technologies allow consumers to live in a connected world with real-time access to information. Technology in the hands of consumers has also enabled the collection of an ever-growing amount of data.

In May 2013 President Obama issued an executive order, "Making Open and Machine Readable the New Default for Government Information," which created the US Government's Open Data Policy and encouraged the release of government data to the public. Between the release of newly-available public data and an increasing amount of data collected from private entities, arose the possibility for re-identification termed the 'mosaic effect.'

A 2014 report by Mathematica Policy Research describes the mosaic effect as "…derived from the mosaic theory of intelligence gathering, in which disparate pieces of information become significant when combined with other types of information." This possibility of re-identification has prompted local, state, and federal governments to re-evaluate and strengthen data anonymization practices.

The global privacy community has responded to the collection of growing amounts of data through regulations aimed at protecting individuals' information, such as the European Union's General Data Protection Regulation (GDPR). GDPR took effect in May 2018 and, in concert with the Data Protection Act of 2018, supersedes the Data Protection Act of 1998. This new regulation broadens the definition of PII and shifts the burden of implementing privacy measures from consumers to companies. The definition of PII under the GDPR is as follows:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

This definition broadly defines what is considered personally identifiable information in relation to EU data subjects. Following suit with the global community's posture to improve individual privacy, the California Consumer Privacy Act (CCPA) took effect in January 2020 and has quickly become the most expansive data privacy regulation in the United States. In November 2020, California passed the California Privacy Rights Act of 2020 (CPRA), which, among other things, creates a standalone agency to administer the state's privacy regulations, imposes new restrictions on cross-context behavioral advertising, and defines a new category of 'sensitive data' within the personal information realm.

As previously discussed, increasing technological advances and a growing amount of consumer data has led to the fixed-element definition of PII becoming a thing of the past. The CCPA, CPRA, and GDPR are leading regulations in this space and lend themselves to the current state of PII, a concept currently in flux. In 2020, 30 US states and Puerto Rico considered some form of data privacy legislation, with some seeing a groundswell for likely adoption in the coming months. At the beginning of 2021, Congress is coalescing around two federal consumer privacy bills. Senator Maria Cantwell introduced the "Consumer Online Privacy Rights Act" (COPRA) in the fall of 2019 which was followed in the summer of 2020 by Senator Roger Wicker's "Setting an American Framework to Ensure Data Access, Transparency, and Accountability" (SAFE DATA) Act. While many fundamental privacy principles are addressed similarly in these bills, there remain specific areas where negotiations continue between interested parties. For the

purposes of this guidebook, it is important to understand that the various sides are at the table and meaningful federal consumer privacy discussions are underway. At the time of publication, these negotiations continue.

The GDPR, CCPA, CPRA, and other regulatory examples not limited to Indiana are of importance in the context of this guidebook as they impose outsized influence on continuing policy development related to privacy and data protection. Taken together, these regulations have set the standard in the European Union and, through California, across much of the US.

**IDENTIFYING RELATED REGULATIONS**

To ensure that users of this guidebook are fully informed, the PII Working Group has attempted to compile a list of all regulations relevant in the data privacy context. While this list relates specifically to data privacy, a more complete list of State and Federal cyber laws has been published by the Legal and Insurance Working Group and is made available via https://www.in.gov/cybersecurity/files/IECC%20Legal%20and%20Insurance%20Working%20Group%20Survey%20of%20Cyber%20Laws.pdf.

- Regulations applicable to business, health providers, and schools
  - Indiana (iga.IN.gov)
    - Persons Holding a Customer's Personal Information, IC 24-4-14
    - Disclosure of Security Breach Act, IC 24-4.9
    - Identity Deception, IC 35-43-5-3.5
  - Federal (https://www.govinfo.gov/app/collection/uscode; https://www.govinfo.gov/app/collection/cfr)
    - Educational
      - Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g
      - Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h
    - Financial
      - Dodd-Frank Wall Street Reform and Consumer Protection Act, P.L. 111-203
      - Fair and Accurate Credit Transactions Act, P.L. 108-159
      - Fair Credit Reporting Act, 15 U.S.C. § 1681
      - Gramm-Leach-Bliley Act, P.L. 106-102, 113 Stat. 1338
      - Protection of nonpublic personal information by financial institutions, 15 U.S.C. § 6801
      - Right to Financial Privacy Act, P.L. 95-630
    - Medical
      - 21st Century Cures Act, P.L. 114-255
      - Confidentiality of Substance Use Disorder Patient Records Rule, 42 CFR Part 2
      - Genetic Information Nondiscrimination Act of 2008, P.L. 110-233
      - Health Insurance Portability and Accountability Act, P.L. No. 104-191, 110 Stat. 1938 (1996)
      - Health Information Technology for Economic and Clinical Health Act, P.L 111-5
    - Telecommunications and Marketing
      - Cable Communications Policy Act, P.L. 98-549
      - Controlling the Assault of Non-Solicited Pornography and Marketing, 15 U.S.C. Ch. 103
      - Children's Online Privacy Protection Act, 15 U.S.C. § 6501-6506
      - Children's Online Privacy Protection Rule, 16 CFR Part 312
      - Telemarketing Sales Rule, 16 CFR Part 310
      - Video Privacy Protection Act, 18 U.S.C. § 2710
- Regulations and related guidance applicable to government
  - Indiana (iga.IN.gov)

        - Fair Information Practices Act, IC 4-1-6
        - Notice of Security Breach, IC 4-1-11
        - Access to Public Records Act, IC 5-14-3
        - Privacy and Disclosure of Bureau of Motor Vehicles Records, IC 9-14-13
        - State of Indiana Information Privacy Policy, https://www.in.gov/mph/files/State-of-Indiana-Information-Privacy-Policy.pdf
    - Federal (https://www.govinfo.gov/app/collection/uscode; https://www.govinfo.gov/app/collection/cfr)
        - Drivers Privacy Protection Act, 18 U.S.C. 2721 et seq.
        - Privacy Act of 1974, 5 U.S.C. § 552a
        - E-Government Act of 2002,
        - Freedom of Information Act, 5 U.S.C. § 552
        - NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
        - NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
        - Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*
        - OMB Circular No. A-130, *Managing Information as a Strategic Resource*
        - OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
        - Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 et seq.

## FUTURE DEVELOPMENTS CONSIDERED

As has been referenced, privacy and data protection continue to be evolving areas of study and regulation. Members of the PII Working Group maintain specialized knowledge in the field and, by discussing next steps in data privacy, hope to peer into the future on a handful of topics for the benefit of the guidebook's users.

### *Data De-identification*

It is important to note that simply because data is labeled as having been 'de-identified' that does not rule out the possibility of reidentification. It is very easy to reidentify data by applying combinatoric algebra and there are many writings on the subject and references to those that have done this. Further, data perturbation, where data is distorted by the de-identification process, distorts the data sets. Unless de-identification is completed using a method that does not distort specific data elements, it is highly likely to occur, lessening the integrity of the data in question. Technologies that can be leveraged to reidentify previously 'deidentified' data will continue to advance. A foundational understanding of what constitutes PII in the singular, collective, and organizationally-specific contexts is key to combatting this.

### *Genomics*

Genomics and precision medicine raise the concern of genomic data being used to identify people, even indirectly. Despite the resulting convictions, recent cases involving GEDmatch and 23andme being used to help identify cold case murderers raised numerous privacy concerns due to law enforcement access to genomics data. While 2008's Genetic Information Nondiscrimination Act created new protections in the health insurance and employment contexts, technological advances are rapidly outpacing data protection regulation in this space.

### *Cross-context Identification & The Mosaic Effect*

There are countless data sources from private-sector brokers to public-sector records, all of which can contribute to concerns relating to cross-context identification and the mosaic effect. Cross-context identification can manifest through Ad Tech's internet and app-enabled behavioral advertising apparatus, which can track you across devices and websites. This is in addition to the voluminous number of data sets available from data brokers, which can be leveraged to form a detailed profile on a specific individual. A recent data breach resulted in the publication of data on more than 120 million households, incorporating street addresses, demographics, and finances for families, as well as information on home and automobile ownership. In a concerning development, this also included information on children.

Beginning with street address, cross-identification can use multiple data sets to produce a more detailed picture of the data subject. Profiles are built using public property information, data about political and charitable donations, and organizational membership activities. The 2020 ransomware attack on Blackbaud contained this information and more in its ResearchPoint application, which allowed the targeting of high-value donors by calculating their net worth and potential ability to donate.

California's recent passage of the CPRA begins to address this in specific contexts. The CPRA defines cross-context behavioral advertising and imposes limitations that target this activity to do-not-sell obligations, while exempting certain analytics functions from the restriction. This illustrates that much of the risk mitigation related to cross-context and mosaic effect identification is best addressed by policymakers. The application of broad protections across sectors of industry and society provide the most significant return when disparate data sources are involved.

### *Vendor Management & Data Protection*

With big-data analytics technologies now the norm, data is a strategic asset for companies and government and must be maintained and protected as such. A contract for services often involves the

exchange of data and information between organizations, potentially including elements of PII. Traditional contract boilerplate documents that protect obvious PII elements like name, address phone number, and email address have become outmoded. Businesses must not only protect the information they maintain on behalf of clients in a cloud solution, but they need to protect their own information as they interact with the third party vendor. This can be achieved through vendor and cloud-specific contract boilerplate terms that explicitly protect organizational assets like data holdings from extra-contractual uses.

Third party systems should also be verified as meeting appropriate cybersecurity thresholds, depending on the type of information planned for the system in question. The Federal Government achieves this through the Federal Risk and Authorization Management Program, or FedRAMP, and state and local governments are able to sign on to a similar program through the non-profit State Risk and Authorization Management Program, or StateRAMP. Alternatively, those contracting must ensure not only adequate data ownership, use, and protection terms, but must expend additional resources to validate the cybersecurity posture of the potential vendor. As organizations shift to a cloud-first posture for IT, programs like FedRAMP and StateRAMP will become all the more important to ensure that data protection is built into contracts and vendor management in an efficient way.

*Payment Card Industry*

The payment card industry continues to evolve and there are expectations that Payment Card Industry-Data Security Standards, known as PCI DSS, will be updated to address cardholder identity management and protection of personal data other than cardholder data. Current PCI standards address identity management only for those with job roles or necessity to access the data, but not for cardholders themselves. Publicly-available information leveraged in conjunction with cardholder data, even if partially redacted, can be used to build user and marketing profiles of individuals. This then can be used to re-identify the users of single-use cards, temporary cards, or virtual card numbers. Many believe that consumer data should be protected as much as credit card data due to potential for misuse and identity theft. The upcoming PCI DSS 4.0 standard makes initial inroads in this area. As the numbers themselves become ephemeral using virtual card numbers, as with the Apple Card for example, the surrounding data becomes the identifying data that can be used to re-identify and enable fraud.

*Blockchain and Distributed Ledger Technologies*

Recently, observers have noted an increasing volume of companies touting the use of Digital Distributed Ledger Technologies and Distributed Verification and Validation Techniques, more commonly referred to as Blockchain, as a privacy-enhancing or security-enhancing technology. This remains in dispute as Blockchain technologies were designed to achieve greater integrity, rather than privacy or security as a whole. For example, blockchain does not allow a user to delete a record, making compliance with various privacy laws difficult or impossible.

To transmit PII, one would need to utilize zero-knowledge proofs or pointers, which remove the distributed verification and validation component and requires both sending and receiving parties to do their own integrity checks. This consumes significantly more resources and energy by removing all PII and replacing it with pointers or zero-knowledge proofs on blockchain.

*Section Conclusion*

This section provides a window into the potential near-term future of data privacy. While many of the covered topics are touched on only briefly, the goal of the PII Working Group is to share a general perspective of this evolving area at the intersection of the law and emerging technologies.

**BEST PRACTICES**

This list offers brief insights and best practices to prepare an organization to be successful in maintaining the privacy of its customers and other stakeholders.

1. Create cybersecurity, internal, and external privacy policies and notices and make them known to all involved. As self-evident as this may appear, some entities do not have internal policies and external-facing notices in place or, if they do, they are not known by those affected.
2. Customers, clients, and website visitors should be made aware of cybersecurity concerns and the efforts being made to address them. Organizations must be transparent about the collection of PII, its use, and procedures that are employed to protect their privacy. Customers/clients must know exactly who to contact (and how) in case of a concern.
3. Conduct regular security audits and privacy impact assessments, or contract to have these conducted, to determine vulnerabilities.
4. Implement a mandatory education and orientation process for all employees who have access to PII. This can be either created in-house or purchased from third-party providers or professionals.
5. Know and follow applicable laws and regulations specific to your industry. In the United States, sector-specific laws regulate data use and/or dissemination in various realms (health, financial, education, etc.).
6. In addition to state and federal law, those who do business internationally are subject to additional sets of rules. For example, the GDPR regulates the collection, use, and transfer of data pertaining to European citizens.
7. In order to transfer data between the European Union and U.S., organizations can join the Privacy Shield Program to self-certify compliance with data privacy regulation in the EU.
8. Monitor or participate in the activities of not-for-profit organizations that promote cybersecurity measures, such as the Center for Internet Security or the All Hazards Consortium. Whether or not their products are purchased, they provide current information via alerts, seminars, and newsletters.
9. Cybersecurity policies should include a plan for informing constituents of any security breach. Best practices require prompt notification.
10. Share information with state and federal authorities. Report not only confirmed data breaches, but possible security incidents and potential threats.
11. Review all cybersecurity and privacy-related policies and procedures at least annually. Like all things pertaining to technology and the law, changes occur constantly. Sample templates for certain, key polices are included with this guidebook as appendices.

## CONCLUSION

This guidebook has been developed for Indiana businesses, small and large, to identify the information in their environment that requires a heightened degree of protection. Across various sectors and individual roles, the collection of PII in systems adds risk to your operation, realized in the context of a security incident or data breach, which cause operational, legal, and reputational harm to businesses. As we've discussed, these risks can be mitigated by collecting only that PII which is required to complete a given transaction.

The PII Working Group has defined and characterized the PII realm, identified regulations related to PII, addressed potential future developments in the practice of privacy and data protection, and has identified practical best practices which organizations are encouraged to apply. After reading this guidebook, you should now be able to call on your understanding of what constitutes PII and how to ensure its appropriate maintenance and use, giving your organization a leg up in today's virtual economy. In the appendices that follow, the PII Working Group has provided sample policies that can be leveraged in the development of your own organizational policies to mitigate cyber threats and enhance the privacy and security of your digital information holdings.

For those of us in government, we serve as stewards of the peoples' information. We strive to maintain that information with an intense focus on privacy and data protection. Apple's Tim Cook is quoted as having said that "…people have entrusted us with their most personal information. We owe them nothing less than the best protections that we can possibly provide." In the business environment of today and tomorrow, that isn't true only for Apple, but for businesses small and large.

**APPENDICES 1-3**

The appendices that follow offer templates that can be leveraged to formulate an internal privacy policy, an information technology policy, and a cyber incident response procedure. While these templates are not intended to replace counsel and guidance tailored to the user's particular challenges or issues, they can serve as a starting point and guide throughout the development process.

**APPENDIX 1**
**[COMPANY NAME] INTERNAL PRIVACY POLICY**
*To the prospective user of this policy Template*:

This policy is to be used internally in your organization. It is different in purpose and content from an *externally* facing privacy notice, like the type that you might post on your website.

There are several reasons you should consider taking the time to utilize this template and to customize it to your business. Chief among those reasons is that this type of policy helps create a culture and environment where your organization treats data with care. That type of culture will help your organization succeed in today's digital business world. In addition, your employees, including management, cannot be expected to understand the role and importance of privacy practices without some guidance, which this policy provides. Management/ownership must provide the policies, procedures and tools to implement the needed rules and expectations to protect data.

This policy template, and the guidance herein, will work with and support your organization's larger data privacy and cybersecurity efforts. That is, this policy will be *one* piece of your overall strategy to protect information.

For additional information about cybersecurity and data privacy, you should consult Indiana's Cybersecurity Hub found at: https://www.in.gov/cybersecurity/

***This policy template is not legal advice and is not a substitute for consulting with a licensed attorney for any particular legal challenges or issues facing your organization. In addition, the larger your organization is in terms of number of employees and/or data handling, and/or the larger its geographic footprint of where it operates, the more likely it is that your organization needs a policy longer and/or more complex than this template, and legal counsel should be consulted.***

---

Version No.: ___ [DRAFT]
Last Updated: [insert date]

1. **Purpose of this Policy**

At [Company Name], we are committed to promoting a work environment and operating the business in a manner that fosters confidence and trust. To accomplish this goal, we must properly manage and protect the Personal Information provided to us by our customers, fellow employees, vendors and suppliers. This Policy sets forth how we will govern and protect that Personal Information.

It is critical that all employees and executives understand that mishandling Personal Information can result in substantial harm to our customers, employees and others. This harm may include financial harm to our company, employees or business partners. The harm may also include identify theft and fraudulent use of information. In addition, mishandling Personal Information can result in serious legal consequences for our organization. Accordingly, compliance with this Policy is mandatory.

2. **Scope**

This Policy applies to all [Company Name] employees, agents, and representatives, including any third–party contractors or third-party provider of services to our company ("Third-Party Provider") who have access to any Personal Information from our company.

This Policy applies to all Personal Information collected, maintained, transmitted, stored, retained, or otherwise used by [Company Name] regardless of where that information is stored and whether it relates to employees, customers, or any other person.

**APPENDIX 1**
**[COMPANY NAME] INTERNAL PRIVACY POLICY**

3. **Definitions**

**"Data Subject"** means the person about whom Personal Information is collected.

**"Personal Information"** means information [Company Name] has collected or otherwise has in its possession that identifies or can be used to identify or authenticate an individual, including, but not limited to:

- Name
- Address
- Telephone number
- Email address
- Employee identification number
- Certain types of particularly sensitive personal information –
  - Social security numbers
  - Driver's license numbers
  - State-issued identification numbers
  - Health insurance identification numbers, such as a Medicare ID
  - Financial account numbers
  - Credit card numbers, or debit card numbers
  - Access codes, personal identification numbers or passwords that would permit access to an individual's financial account
  - Medical or health information

If you have any questions about whether any information qualifies as Personal Information ("**PI**"), you should contact [CONTACT NAME].

**"Security Incident"** means any act, omission, event or circumstance that compromises or *potentially* compromises the availability, confidentiality, integrity or security of PI.

4. **Using and Retaining Personal Information**

Notice and Collection. It is our company's policy that whenever we collect PI for any purpose, including for human resources or employment purposes, we will inform the Data Subject of how we will use, disclose, retain and/or discard that PI by presenting (or at least making available) a privacy policy or privacy notice to the individual at the time they provide the information.

We will only collect PI in compliance with applicable company policies, notices, and/or Data Subject consent. PI collected must be limited to that which is reasonably necessary to accomplish [Company Name]'s legitimate business purposes or as necessary to comply with law.

Access, Use and Sharing. Employees may only access PI when that information relates to and is necessary to perform their job duties. You may not use PI in a way that is incompatible with this Policy or the notice given to the Data Subject at the time the information was collected. If you are unsure about whether a specific use or disclosure is appropriate, you should consult with [Contact Name]. You may only share such information with another Company employee, agent, or representative if the recipient has a job-related need to know the information.

PI may only be shared with a Third-Party Service Provider if it has a need to know the information for the purpose of providing the contracted services and if sharing the PI complies with any privacy notice provided to the Data Subject. You may not share PI with a Third-Party Service Provider without prior

written supervisor approval and/or a fully executed written contract that provides the appropriate safeguards for the information at issue.

Accuracy. It is important that PI that the company collects, maintains, and uses is accurate, complete, and relevant to the purposes for which it was collected. Employees should report inaccurate PI to their supervisor.

Security. All employees are responsible for doing their part to help protect PI. [Company Name]'s Information Technology ("IT") and/or Information Security ("IS") personnel have implemented certain technical, administrative and physical safeguards for the protection of PI. Employees must follow those security procedures at all times. You must exercise particular care in protecting the types of *sensitive* PI listed above in this Policy from loss, unauthorized access and unauthorized disclosure.

Retention and Disposal. PI should be kept only for the amount of time it is needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. Employees must follow the applicable records retention schedules and policies related to retention and destruction of devices and/or media containing PI.

## 5. **Training Employees and Supervising Contractors**

All [Company Name] personnel who have access to PI will be trained on this Policy and are expected to abide by it. The company also expects that employees will help ensure that PI entrusted to a Third-Party Service Provider is protected by appropriate contract provisions. Personnel with responsibility for supervising employees or managing Third-Party Service Provider relationships will be trained on how to carry out these duties.

## 6. **Reporting a Security Incident**

If you know or suspect that a Security Incident has occurred, do not attempt to investigate the matter yourself. Immediately contact [CONTACT NAME] [and/or follow the company [SECURITY INCIDENT RESPONSE PLAN/PROCEDURE]].

## 7. **Monitoring Compliance and Enforcement**

[CONTACT NAME] is responsible for overseeing management and enforcement of this Policy. If you are concerned that any provision of this Policy, or any related policy, operating procedure, process, or guideline designed to protect PI, has been or is being violated, please contact [CONTACT NAME]. The company may conduct reviews or audits to assess compliance with this Policy. Employees who violate this Policy and any related guidelines, operating procedures, or processes designed to protect PI may be subject to discipline, up to and including termination.

Other [Company Name] policies also apply to the collection, use, storage, protection, and handling of PI and may be relevant to implementing this Policy. You should familiarize yourself with these policies, including: [LIST OF OTHER APPLICABLE POLICIES]

[Insert line for name, signature, and date, if organization desires that this form be signed to acknowledge receipt.]

**APPENDIX 2**
**[COMPANY NAME] INFORMATION TECHNOLOGY POLICY**
*To the prospective user of this policy Template*:

This policy is to be used internally in your organization. There are several reasons you should consider taking the time to utilize this template and to customize it to your business. Chief among those reasons is that this type of policy helps create a culture and environment where your organization treats data with care. That type of culture will help your organization succeed in today's digital business world. In addition, your employees, including management, cannot be expected to understand the role and importance of privacy and security practices without guidance. Management/ownership must provide the policies, procedures and tools to implement the needed rules and expectations to protect data.

This policy template, and the guidance herein, will work with and support your organization's larger data privacy and cybersecurity efforts. That is, this policy will be *one* piece of your overall strategy to protect information.

For additional information about cybersecurity and data privacy, you should consult Indiana's Cybersecurity Hub found at: https://www.in.gov/cybersecurity/

***This policy template is not legal advice and is not a substitute for consulting with a licensed attorney for any particular legal challenges or issues facing your organization. In addition, the larger your organization is in terms of number of employees and/or data handling, and/or the larger its geographic footprint of where it operates, the more likely it is that your organization needs a policy longer and/or more complex than this template, and legal counsel should be consulted.***

---

Version No.: ___ [DRAFT]
Last Updated: [insert date]

## 1.0 Overview, Purposes of this Policy, and General Provisions

[Company Name] ("Company")'s computers, computer networks, other information technology ("IT") resources, and communications systems and equipment are provided to employees to help them perform their job duties and assist the organization achieve its business objectives. However, providing these resources raises potential risks for Company, including loss or misuse of Confidential Information, and/or data breach of company data, all resulting in potential legal consequences for Company and/or its employee(s). Therefore, to protect Company and its employees, this Policy restricts the use of all IT resources, communications systems and equipment as described below.

The resources covered by this Policy are provided for business use only, subject to the limited exceptions addressed below. Each employee is responsible for complying with this Policy and using these resources and systems in a productive, ethical, and lawful manner.

Company's policies prohibiting harassment apply to the use of the company's IT and communications systems. Employees may not use any IT or communications system in a manner that may be construed as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by federal, state, or local law.

The use of Company's IT and communications systems by an employee shall signify his or her understanding of, and agreement to comply with, this Policy.

### 1.1 Administration of this Policy

**APPENDIX 2**
**[COMPANY NAME] INFORMATION TECHNOLOGY POLICY**
[Contact Name] has primary responsibility for administration of this Policy. If you have questions regarding this Policy, please contact [Contact Name].

### 1.2 Resources and Systems Covered by This Policy

This Policy governs all IT resources (both hardware and software) and communications systems (both hardware and software) that are owned by or made available by Company. All of these IT and communication resources, systems and equipment (collectively "IT SYSTEMS") include but are not limited to:

- Email systems and accounts
- Internet and intranet access
- Telephones and voicemail systems, including wired and mobile phones, smartphones, and pagers
- Printers, photocopiers, and scanners
- Fax machines, e-fax systems, and modems
- Computers, computer networks, and communications systems, hardware, peripherals, and software, including network key fobs and other devices
- Portable storage devices
- Cloud-based accounts and software
- Closed-circuit television (CCTV) and all physical security systems and devices, including access key cards or fobs
- Electronic systems on or within company vehicles.

This Policy also applies to and governs an employee's own computers, electronic devices, equipment, software, apps, and/or accounts if and to the extent that an employee uses them to conduct Company's business or to access Company's IT SYSTEMS.

### 1.3 No Expectation of Privacy

All IT SYSTEMS and the contents of the IT SYSTEMS, including but not limited to items listed in this Policy, are the property of Company and not the employee. Employees should have no expectation of privacy whatsoever in any message, file, data, document, facsimile, telephone conversation, social media post, conversation, or any other kind or form of information or communication transmitted to, received, or printed from, or stored or recorded on the company's IT SYSTEMS.

*Do not use the company's IT SYSTEMS for any matter that you desire to be kept private or confidential from the company.*

### 1.4 Network Systems – Access Is Limited by Authorization

Company maintains integrated IT SYSTEMS to facilitate all aspects of its business. You may never sign on to any network equipment using the password or user name of another employee. No employees

should access, attempt to access, alter or delete any file, information, document or data except in furtherance of *authorized* job duties.

### 1.5 Confidentiality and Proprietary Rights

Company's Confidential Information and intellectual property (including trade secrets) are extremely valuable. Use or disclosure of such Confidential Information to anyone outside our company is prohibited. Do not use Company's name, brand names, logos, taglines, slogans, or other trademarks without written permission.

### 1.6 Inappropriate Use of IT Resources and Communications Systems

You are never permitted to use the IT SYSTEMS for any inappropriate or unlawful purpose. This includes but is not limited to:

- Misrepresenting yourself as another individual or company
- Sending, posting, recording, or encouraging receipt of messages or information that a reasonable person would find offensive or demeaning toward an individual or group because of a protected characteristic, including but not limited to sexual, racist, or religious content
- Revealing Company's proprietary or Confidential Information, including business information that an employee does not have a right to disclose as described in this Policy, or intellectual property without authorization
- Conducting or soliciting illegal activities
- Representing your personal opinion as that of Company
- Interfering with the performance of your job or the jobs of other Company employees
- For any other purpose that violates Company policies or practices

## 2.0 Discipline, Civil and Criminal Liability For Violations of this Policy

Employees who violate this Policy are subject to discipline, up to and including termination of employment.

## 3.0 Rules and Guidance for Specific Issues, Uses, Applications or Hardware

Below, Company addresses many common concerns, risks and issues that arise in the modern workplace. If a question arises that is not addressed in this Policy, employees should seek guidance from [Contact Name].

### 3.1 Connecting to the IT SYSTEMS Remotely

If an employee is granted access to connect to the IT SYSTEMS from home or otherwise via a personal device, it is the employee's responsibility to maintain reasonable cybersecurity on their personal computer or other device(s) they are using to connect. At a minimum, that includes up to date antivirus/antimalware software, and maintaining all software updates as issued.

### 3.2 Email, Text Messaging, and Other Messaging Applications or Apps

Company provides certain employees with access to email, text messaging systems and/or other messaging applications for use in connection with performing their job duties efficiently and effectively. This Policy strives to ensure that these communication tools do not compromise security and remain in compliance with Company's other policies.

3.2.1 Etiquette.

Proper business etiquette must be maintained when communicating via electronic means. Sarcasm, inappropriate comments and attempts at humor should be avoided. Electronic communications allow no facial expressions and voice tones to assist in determining the meaning or intent behind comments. To avoid offending a coworker or customer, be professional and respectful in correspondence.

3.2.2 Links and Attachments

Malicious links and attachments are common sources of viruses and other malicious software. Employees may not click on links or attachments that the employee was not expecting. If in doubt, employees should call the sender (not via a phone number obtained from the communication at issue) to verify if the link or attachment is legitimate. This applies to text messages and any other application to which the employee has received a link or attachment.

3.2.3 Safety

Employees may not read or send emails, text or other electronic messages related to Company while operating any motor vehicle, or read or send email, text or other electronic messages of any kind (personal or professional) while operating a Company- owned vehicle.

3.2.4 Spam.

Employees may receive unsolicited commercial or bulk messages (spam) which is a nuisance, a drain on resources, and may spread malware. Do not open unsolicited messages and report suspicious messages to [Contact Name]. Do not reply to spam messages in any way. Do not attempt to "unsubscribe" from its distribution list. For assistance blocking spam messages, contact [Contact Name].

3.2.5 Email Use and Storage Restrictions For Sensitive Information

It is common for email accounts, including corporate accounts, to be breached by outside hackers. In addition, a "regular" email sent over the internet to reach its destination generally lacks the security protections needed for sensitive information. Accordingly, in order to help prevent data breaches and protect both Company data and the identities of its employees, customers and others, the following rules apply.

Employees may not send a regular email that includes (in the email itself or in any attachment) more than:

- *Last 4 digits of any Social Security Number*
- *Last 4 digits of any Driver's License Number*
- *Last 4 digits of any State Identification number*
- *Last 4 digits of any credit or debit card number*
- *Last 4 digits of any financial account number*

Employees may not store emails in their inbox, inbox subfolders, sent or deleted mail that contain any of the types of data listed above in its full form (i.e., more digits than listed above).

If an employee needs to send any of the types of sensitive information noted above in its full form, the employee should see [Contact Name] for assistance with more secure methods.

3.2.6 Personal Use of *Company-Provided* Email. Company recognizes that employees may occasionally desire to use their company-provided email account for *personal* use while at the office or by means of the Company's IT SYSTEMS. Use of your Company email account to conduct purely personal business is discouraged, and should be done sparingly, if ever. If an employee needs to do so in unusual circumstances, it is permitted so long as it is during non-work time (for example, breaks or meal periods), does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity.

3.2.7 Use of *Personal* Email Accounts. Company recognizes that employees might occasionally need to access and/or use their personal email accounts for *personal* use while at the office via the IT SYSTEMS. Such occasional use is permitted so long as it is during non-work time (for example, breaks or meal periods), does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. In addition, the following rules apply when accessing your personal email account:

- You may not conduct any Company business or your job duties via your personal account.
- Do not click on any unexpected links or attachments, or open files, within a personal email account, unless you have confirmed their trustworthiness.
- Never send any of Company's information, documents or data of any kind to or from your personal email account.

### 3.3 Flash Drives/Portable Hard Drives

Portable electronic storage devices present a considerable risk because they can be easily lost or stolen. Accordingly, extra care is required to protect Company and therefore:

- Employees may not save any of Company's business related data to an *unencrypted* flash drive or portable hard drive.
- Employees may not save the types of information listed in Section 3.2.5 above to any such device.
- Employees may not use personal flash drives or personal hard drives with Company's IT SYSTEMS, as they present a risk of spreading malware.

### 3.4 Installation of Software or Applications / "Apps" and Disabling Software

Employees may not download or install any software, application ("app") or program to any Company-issued equipment (desktop computer, laptop, iPad, tablet, smart phone, or any other Company-issued device) unless such action is authorized in writing by [Contact Name]. Employees may not download games or any other non-work related files to any Company-issued equipment.

Employees may not disable any software, even temporarily, without permission from [Contact Name].

### 3.5 Laptop Use

Laptops require additional care because they can be easily lost or stolen. All Company laptops should be set up with an encrypted hard drive. Employees may not download or install any software, applications, "apps" or programs to a Company-owned laptop without written approval by [Contact Name]. Employees are strongly discouraged from leaving laptops in motor vehicles, but if they must do so, they should be left in the locked trunk of the vehicle or, if there is no trunk, they should be kept out of sight in a locked vehicle (example, under a blanket in the back of an SUV).

Employees may not save any Company work-related information to a *personal* laptop.

### 3.6 Logging Out of the Network and Devices

Screen saver passwords, also known as "workstation timeouts" or "lock screens," secure Company's Confidential Information by protecting active computer sessions when you step away. Locking screen savers must activate after a maximum inactivity time of ___minutes. If you handle highly Confidential Information, you should lock your screen any time you leave it unattended. Employees must log out of Company's computer network entirely at the end of each workday.

Employees should see [Contact Name] if they need assistance to comply with these requirement.

### 3.7 Passwords

Employees' passwords must comply with Company's requirements as to length, complexity, and periodic password change.

Employees may not share user names, passcodes or passwords with any other person, except to the extent needed with administrative assistants and/or IT staff. Employees shall immediately inform [Contact Name] if they know or suspect that any user name, pass code, or password has been improperly shared or used, or that IT security has been violated in any way.

### 3.8 Personal Cloud and Personal Applications

Employees may not use any personal cloud-based account of any application, "app" or service to upload, transmit, store, share or work on any of Company's business information. This includes any such account that is set up only in the employee's name, even if the employee used their Company email address with the account. If this type of service is needed, the employee must use a/the Company's approved business account.

Similarly, employees may not use personally downloaded applications ("apps"), on any device or computer, to conduct their job duties or to transmit, store, upload, share or work on any of Company's business information.

### 3.9 Smart Phones/ Cell Phones

[Insert company-specific rules based upon whether your company: allows or encourages Bring Your Own Device (BYOD), or provides company issued phones (and/or other mobile devices), or some combinations of both. Insert here specific rules for each category of use that your company permits, based upon the nature how devices will be used for work, the sensitivity of the data involved, and other pertinent factors.]

**APPENDIX 2**
**[COMPANY NAME] INFORMATION TECHNOLOGY POLICY**

## 4.0 Internet Use

Company provides internet access to certain employees for use in connection with performing their job duties. The following outlines the expectations regarding internet use by employees.

Company recognizes that employees might work long hours and occasionally may desire or need to access the internet for personal activities at the office or by means of the company's IT SYSTEMS. Such occasional use is authorized so long as it is during non-work time (for example, breaks or meal periods), does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity, and does not compromise Company's Confidential Information of the proper operation of its IT SYSTEMS.

Using the internet to access pornographic, sexually explicit, or "hate" sites, or any other website that might violate law or Company policies against harassment and discrimination is never permitted.

## 5.0 Responding to Suspicious Computer Activity, Pop-Ups or Threats

Malicious actors are constantly creating new tricks and schemes to try to get computer users to click on links, open attachments, or do other acts that will infect their computer network with malicious code or result in the fraudulent transfer or payment of money. This may include pop-ups messages that appear to take over a user's computer, or emails that attempt to blackmail a user.

Employees should not ever engage, call or agree to pay the sender of any such trick or scheme. If an employee has any doubts about an email, pop-up ad or error message of any kind, the employee should not try to handle it themselves but should instead reach out to [Contact Name] for assistance.

[Insert line for name, signature, and date, for employee if organization desires that this form be signed to acknowledge receipt.]

**APPENDIX 3**
**[COMPANY NAME] CYBER INCIDENT RESPONSE PROCEDURE**
*To the prospective user of this template procedure*:

This procedure is for internal use in your organization. The potential effectiveness of this procedure will depend on the extent to which you invest the time to customize it to your business and train those involved in its use.

This procedure template, and the guidance herein, will work with and support your organization's larger data privacy and cybersecurity efforts. That is, this procedure will be *one* piece of your overall strategy to protect information.

For additional information about cybersecurity and data privacy, you should consult Indiana's Cybersecurity Hub found at: https://www.in.gov/cybersecurity/

***This procedure template is not legal advice and is not a substitute for consulting with a licensed attorney for any particular legal challenges or issues facing your organization. In addition, the larger your organization in terms of the number of employees and/or data handling, and/or the larger its geographic footprint of where it operates, the more likely it is that your organization needs a procedure which is more complex than this template, and legal counsel should be consulted.***

Version No.: ___ [DRAFT]

Last Updated: [insert date]

## I. Objectives and Scope

This [Company Name] Cyber Incident Response Procedure governs all employees and management on how to respond to a potential or actual cybersecurity threat or incident ("Security Incident").

This Procedure aims to prevent incidents from going unnoticed or unreported, which may result in the magnitude of harm associated with that or a future incident being significantly greater than if the activity was promptly noted and addressed.

This Procedure also aims to make responding to Security Incidents a standardized procedure, which will be beneficial for both the speed of response and will prevent costly mistakes.

All company employees, including management, must be familiar with, and abide by this Procedure.

## II. Incident Response Team

The [Company Name] Incident Response Team ("IRT") is established and certain roles and responsibilities assigned below to achieve an orderly and professional response to Security Incidents.

The IRT is composed of the following employees, who are all IRT members, whether they are listed as a Team Member or as a Designated Backup:

| Team Member | Designated Backup |
|---|---|

| | |
|---|---|
| [Team Member 1] / IT "Help Desk" - This is your internal or external computer "Help Desk" or other IT personnel you use for routine computer issues. | If the resource used as your computer "help desk" is only one person, you should designate someone else here as their backup. |
| [Team Member 2] | [Team Member 3] |
| [Team Member 4] This should be a high-ranking member of management or an owner. | [Team Member 5] This should be a high-ranking member of management or an owner. |

*The Designated Backups are critical team members so that this Procedure will still work even when another IRT member is on vacation or otherwise not available.*

*All IRT members shall keep a hard copy of this Procedure with them at the office and their home for ready access during times when the computer network and/or network communication systems are down. Contact information for IRT members is listed at the end of this Procedure.*

## III. Definitions

It is important that all company employees understand that not all potential or actual cybersecurity incidents or events are a "data breach." In general, neither employees nor management should refer to any incident as a "data breach" (unless approved by legal counsel), because use of that term carries with it legal conclusions and related legal obligations.

"**Security Incident**" is a very broad term for purposes of this Procedure and means any event, incident, act, omission that a company employee or member of management becomes aware of *which could possibly be a threat* to the company computer system, any device connected to the system, or any company information. Examples of potential "Security Incidents" include, but are *not limited to*:

- Unusual Error Message on Your Computer or other Electronic Device or Phone
- Suspicious Email or Email Attachment
- Unusual Computer Behavior or Performance
- Blackmail Threat Received via Email or other Electronic Means
- Unusual Pop-Up Messages, Including Ones that Claim Your Computer is "Infected"

"**Data Breach**" is a legal conclusion that, depending on the applicable law, certain type(s) of information have been accessed, acquired or compromised such that a legal obligation has been triggered to notify one or more parties of the event and/or to notify a governmental authority.

## IV. Reporting Security Incidents

Any employee who discovers or encounters even a *potential* Security Incident should contact Help Desk immediately. It is important that employees report even issues that they believe are minor, because it will provide information to the IRT of what is happening across the Company and ensure that the IRT verifies that what looks like a minor issue is actually so. The employee reporting the issue will pass along basic information, such as:

- Their name

- Contact information
- The nature of the concern
- The equipment or persons involved along with their location
- How the issue was detected
- When the issue was first noticed

## V. IRT Response Procedures

### A. Initial Assessment and Instructions

1) If Help Desk determines that the issue is a routine matter, Help Desk will proceed with guiding the employee on what to do next. This might include advice on situations such as directing an employee what they should do with a suspicious email.

2) If Help Desk determines that the issue may be beyond a routine matter, Help Desk will contact [Team Member 2] immediately.

Once [Team Member 2] (*or his/her backup - [Team Member 3]*) receive the call from Help Desk, they will assess the situation, including:

- What type of threat is it?
- Is it ongoing?
- Is the affected equipment business critical?
- What is the severity of the potential impact?
- Name of system being targeted, along with operating system, IP address, and location.
- What types of information may be targeted or at risk?

3) Help Desk and [Team Member 2] (or his/her backup - [Team Member 3]) will give instructions to the employee regarding any immediate action the employee should or should not take. For example, they may instruct the employee to take actions such as to unplug the device from the network or disconnect from Wi-Fi.

If Help Desk and [Team Member 2] (or his/her backup [Team Member 3]) determine this is an issue that can be handled in-house, they will proceed to do so. If instead, they determine that the issue may require outside help, they will proceed to step B below.

### B. Escalation Step 1 – Initial Meeting

If Help Desk and [Team Member 2] recognize the Security Incident as being potentially serious or beyond (or likely beyond) internal capabilities, they will immediately contact Team Member 4 (or his/her backup [Team Member 5]).

Help Desk,[Team Member 2] (or backup) and Team Member 4 (or his/her backup – [Team Member 5] will meet in person or by telephone to determine next steps, including whether it may be appropriate to contact the company's cyber insurance carrier and any other insurance carrier that might need to be put on notice. Topics for this/her discussion will include:

- Nature of the event/incident

- Is the incident still in progress?
- What data or property is threatened and how critical is it?
- What is the potential impact on the data?
- What is the potential impact on employees and customers?
- What system or systems are targeted, where are they located physically and on the network?
- Is the response urgent?
- Can the incident be contained and remediated with internal resources?
- Is there a need for professional outside help to preserve evidence?
- Is there a potential need for law enforcement to be involved?

### C. Escalation Step 2 – Getting Outside Help

If the Escalation Step 1 Initial Meeting results in a determination that the situation warrants calling for outside help, the IRT shall immediately call the company's outside legal counsel who has been designated in advance to respond to cyber incidents, or the company's cyber insurance carrier, whichever has been pre-arranged as the appropriate "first call" to make.

The IRT will then coordinate with and support outside legal counsel and/or the cyber insurance carrier's breach response team.

## VI. Post Incident Procedures

For each event that rises beyond the initial step of being quickly resolved by Help Desk, the following information shall be documented by the IRT to help improve cyber defenses and this Procedure going forward:

1. A description of the incident, with pertinent details.
2. How the incident was discovered.
3. The category of the incident -
    a. Minor – handled *easily* in-house
    b. Moderate – handled in-house
    c. Severe – outside help required
4. How the incident occurred, whether through email, firewall, etc.
5. Where the attack came from, if known, such as IP addresses and other related information about the attacker.
6. What was done in response?
7. Whether the response was effective, and if not, why not.
8. Cost of the incident.

The IRT, with the assistance of legal counsel, will help ensure evidence is preserved as appropriate, such as copies of logs, emails and other communication, and metadata for any possible or anticipated insurance claims, investigations, civil claims or prosecutions.

After an incident is resolved, the IRT will update this Procedure as needed. The IRT will review and update this Procedure at least annually.

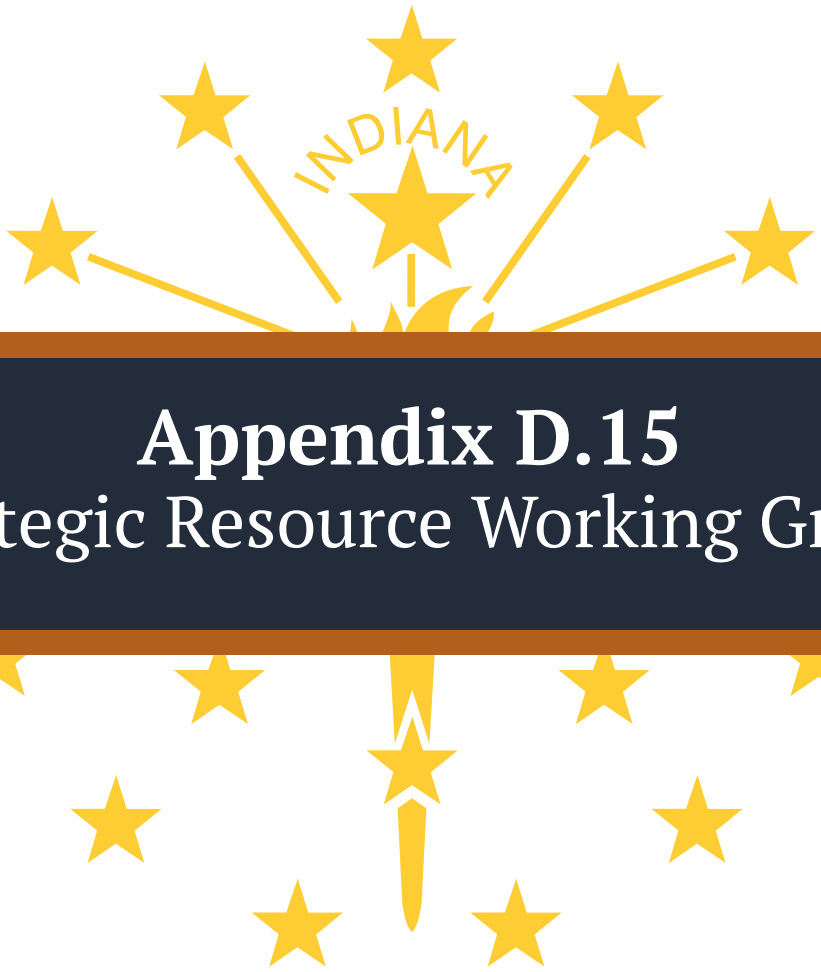
## VII. Contact Information

The following phone numbers are for contacting all IRT members (including backups) away from the office in the event of an incident:

| Name | Mobile Phone | Home Phone |
|---|---|---|
| Team Member | | |
| Team Member | | |
| Team Member | | |
| Team Member | | |
| Team Member | | |
| Team Member | | |
| Cyber Insurance Carrier | | |

The following law-enforcement resources contact information may also be needed:

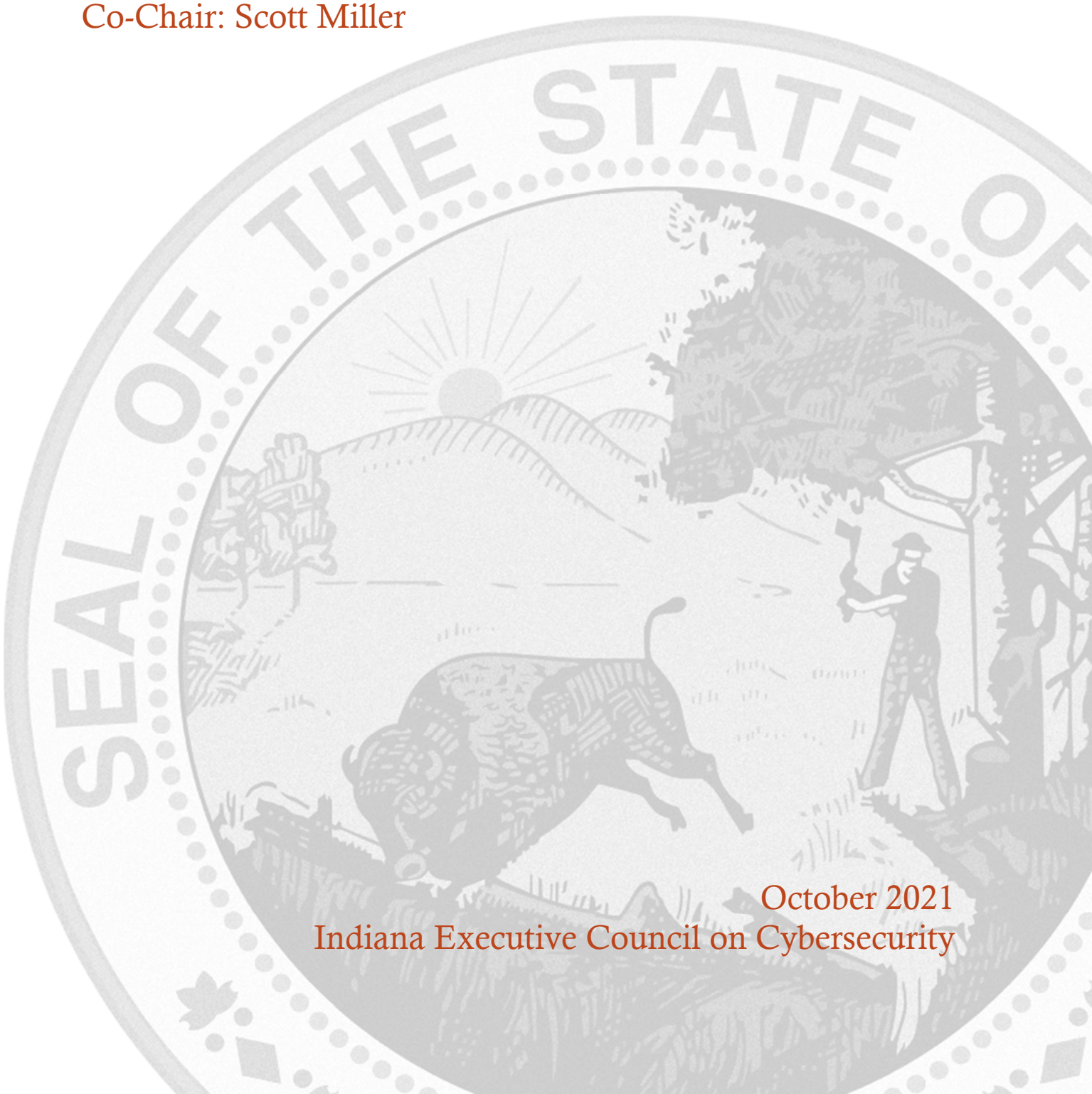
- FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field
- FBI's Internet Crime Complaint Center (IC3): http://www.ic3.gov
- Indianapolis Field Office of Federal Bureau of Investigation (FBI): (317) 595-4000
- Indiana State Police, Cybercrime & Investigative Technologies Section. More information can be found at: https://www.in.gov/isp/3234.htm
- U.S. Secret Service, Financial Crimes Task Force (FCTF): 317-635-6420
- U.S. Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices




# Appendix D.15
## Strategic Resource Working Group

# STRATEGIC RESOURCE WORKING GROUP STRATEGIC PLAN

Chair: Chetrice Mosley-Romero
Co-Chair: Scott Miller




October 2021
Indiana Executive Council on Cybersecurity

# Strategic Resource Working Group Plan

# Table of Contents

# Committee Members

## Committee Members

| Last Name | First Name | Organization | Title | Member Type (Chair/Co-chair/Full-time, As needed) |
|---|---|---|---|---|
| Ayers | David | Indiana Office of Technology | Program Communications Manager | Chair Proxy |
| Banta | Rich | Lifeline Datacenters | Principal & Chief Information Security Officer | Full Time |
| Beard | Amy | Indiana Department of Insurance | Commissioner | As Needed |
| Best | Gerald | Astro Logistic Solutions | Managing Director | As Needed |
| Creech | Bill | Cadre Information Security | Enterprise Sales Manager | As Needed |
| Cudby | Joe | MXL Consulting | Chief Executive Officer/Principal | Full Time |
| Dietz | J. Eric | Purdue University | Professor-Computer and Information Technology | As Needed |
| Dittmer | Robert | Government Performance Solutions, LLC | Senior Consultant | Full Time |
| Goldsmith | Reid | Indianapolis International Airport | Senior Director Information Technology | Full Time |
| Guarente | Tom | DeepInstinct | Americas Vice President | Full Time |
| Huston | Jim | Indiana Utility Regulatory Commission | Commissioner | As Needed |
| Hyer | Sam | Indiana Governor's Office | Senior Operations Director | As Needed |

| | | | | |
|---|---|---|---|---|
| LaChat | Owen | Northwest | VP,Technology Infrastructure and Security Management | As Needed |
| Langelier | Mike | TechPoint | President | As Needed |
| Lewis | Landon | Pondurance | Chief Executive Officer | As Needed |
| Loepker | Mark | Insure | Director | As Needed |
| Lowden | Rob | Indiana University | Chief Information Officer | As Needed |
| Mackey | William | Indiana State University | Instructor | Full Time |
| McGuinness | Joe | Indiana Department of Transportation | Commissioner | As Needed |
| Miller | Scott | Citizens Energy Group | Manager of Security and Compliance | Co-Chair |
| Mosley-Romero | Chetrice | State of Indiana | Program Director | Chair |
| Newman | Anthony | Purdue University | Chief Information Security Officer | As Needed |
| O'Hara | Brian | BTO Associates, LLC | President/CEO | Full Time |
| Owen | Dan | Sexton's Creek | Associate | As Needed |
| Phelps | Tasha | Phelco Technologies, Inc. | President | Full Time |
| Roeder | John | Lt. Governor's Office | Director of Legislative Affairs & Parliamentarian | As Needed |
| Rupel | Johnathan (CPT) | Raytheon | Cyber Engineer | Full Time |
| Xu | Dongyan | Purdue University | Director-CERIAS and Samuel Conte Professor of Computer Science | Full Time |

# Introduction

# Introduction

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.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

# 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)
  - Conferences
  - Webinars
  - Best Practices/Examples of other Councils and Boards
  - Feedback from Council members
  - INSuRE Program
  - Presidential Executive Order
  - National Conference of State Legislators Cybersecurity Taskforce Resources and Whitepapers

- **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
      - https://nfcausa.org/
      - https://www.dhs.gov/national-network-fusion-centers-fact-sheet
      - 2018-to-2021-National-Strategy-for-the-NNFC7715.pdf (wpengine.com)
    - 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 Awareness and Sharing Working Group
    - National Guard cyber strategy and capabilities
    - IDHS cyber strategy and capabilities
    - Federal partnerships
    - In our research, we were unable to find a comprehensive, deep analysis of federal and state policy around cybersecurity from 2011-2021, 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.

- **2021 Working Group Deliverables**
  - Policy Research Report
  - IECC Scorecard 2.0
  - Indiana State of Cyber Report 2017-2021
  - IECC Strategic Plan - 2021
  - Outreach to Underrepresented Sectors

- **References**
  - NGA Meet the Threat - https://www.nga.org/cms/meet-the-threat
  - National Association of State Chief Information Officers (NASCIO) - https://www.nascio.org/
  - 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
  - Cyber Disruption Response Planning Guide - NASCIO
  - Building a Cybersecurity Workforce Pipeline - National Governors Association
  - 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
  - Congressional Cybersecurity Caucus
  - MS-ISAC (Multi-State Information Sharing & Analysis Center)

- **Additional Notes**
  - **State and Other Example Websites**
    - Cyber Virginia
    - Michigan Cyber Initiative
    - Missouri Office of Cybersecurity
    - Pennsylvania
    - DET Cybersecurity Strategy 2017 (wi.gov)
    - Multistate Information Sharing and Analysis Center (MS-ISAC)

# Research

# Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
   a. Governor established Indiana Executive Council on Cybersecurity – March 2016
   b. Crit-Ex 2016
   c. Governor continued Indiana Executive Council on Cybersecurity – January 2017
   d. Developed and implemented the 2018 State Cybersecurity Strategic Plan by the Indiana Executive Council on Cybersecurity
   e. 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. 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.
      - An education on the topic of cybersecurity with policy makers is needed on a local, state, and federal level.

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
      - DET Cybersecurity Strategy 2017 (wi.gov)
      - Multistate Information Sharing and Analysis Center (MS-ISAC)
      - 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 - 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.**
   - National Governors Association
   - National Association of State Chief Information Officers (NASCIO)
   - Purdue Homeland Security Project – in progress
   - State-to-State Comparison Research – ongoing
   - Cybersecurity Prediction Reports
   - Fusions Centers
   - Information Sharing and Analysis Centers (ISACs)
   - Indiana Department of Homeland Security/United States Department of Homeland Security (IDHS/USDHS)
   - Policy
   - Conferences
   - Webinars
   - Best Practices/Examples of other Councils and Boards
   - National Governors Association Whitepapers
   - State-to-State Examples
   - INSuRE Program participation
   - Presidential Executive Orders
   - The National Conference of State Legislators Cybersecurity Taskforce provides policy makers a variety of resources online.

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.
   b. Complete an analysis of federal policy related to cybersecurity since 2011 and any federal acts that affect cybersecurity today.
   c. Complete an analysis of state policies the last five years that have passed or been debated.
   d. Increased understanding and awareness of cybersecurity threats with state and local governments.
   e. Assist in providing guidelines and resources that encourage safer municipality, corporate, and personal practices that protect the state's infrastructure 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. 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. Through https://www.cyberseekin.org/ we can see the state's cybersecurity supply and demand; pathways showing common roles within cybersecurity and transition opportunities; and training opportunities.

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 since critical infrastructures are securing their operations and data not only physically but through technology as well.

12. **What are your communication protocols in a cyber emergency?**
    a. The State of Indiana has developed a Cyber Incident Response Plan and we offer additional resources to assess your cybersecurity preparedness, including the Indiana Cybersecurity Scorecard. In addition, in 2021 Indiana lawmakers recently passed legislation that will increase the amount of information sharing regarding cyberattacks and other threats across state agencies and local government. This new law requires public-sector entities to report incidents such as ransomware, software vulnerability exploitations, denial-of-service attacks and more.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. See sector specific questionnaires in each of the other 14 strategic plans.

# Deliverable: Policy Research Report

# Deliverable: Policy Research Report

## *General Information*

1. **What is the deliverable?**
   a. An update to the State and federal updated research report on cybersecurity legislation that was completed in 2018.

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?**
   ☐ 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. Compiling the policies and legislation that have been introduced since 2018 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?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. Perhaps the research done by the National Conference of State Legislators (https://www.ncsl.org/) may have research that overlaps 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?**
    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. State of Indiana Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. Being able to complete a comprehensive analysis with limited resources.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Select a resource to complete updated research report | Cybersecurity Program Director | 0 | January 2022 | Selected INSuRE Partner |
| Conduct research and utilize a tool to use for future policy analysis | INSuRE Program Partner: University of Alabama | 0 | February – November 2022 | Cybersecurity Program Director will serve as the Technical Director of the project |

| | | | | |
|---|---|---|---|---|
| Final report and tool completed | INSuRE Program Partner: | 0 | December 2022 | |
| Provide IECC with final report and access to tool | Cybersecurity Program Director | 0 | December 2022 | |
| 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 | |
| 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?**

☐No ☒ Yes

| 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?**

| 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 continues to stay current and consider possible policy recommendations, it is imperative that we understand what policy or policies have been discussed, passed, and/or failed in all 50 states and at the federal level from 2011 - 2021. This will help assure we understand these recommendations in the proper context and communicate 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 are 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 a 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 updating and completing this deliverable is creating a policy that is not well informed, and it increases the possibility of unintended consequences to 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?**

☐No ☒ Yes

**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?**

☒No ☐ Yes

a. No state has a publicly published review of all cyber legislation introduced from 2011-2021. 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?**

☒No ☐ Yes

**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 Cybersecurity Program Director will work with the INSuRE program to initiate the process of identifying a resource for completing the updated report.

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

a. All sectors can benefit

## 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)?**

☒No ☐ 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 update a report of state and federal cybersecurity legislation by December 31, 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: IECC Scorecard 2.0

# Deliverable: IECC Scorecard 2.0

## *General Information*

1. **What is the deliverable?**
   a. IECC Scorecard 2.0 – More specifically, providing a guide to go along with the Scorecard so that an organization can begin the process of deciding what things they can do to improve their cybersecurity posture.

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?**
   ☐ 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. In its current form, it serves a baseline as a measurement of the effectiveness of the IECC deliverables as well as a more detailed cybersecurity self-assessment. Secondly, it provides a starting place with some high-level direction of how to "level up."

6. **What metric or measurement will be used to define success?**
   a. In addition to completing the Scorecard Level Up Guide, there will be a sampling of local governments who will be completing the scorecard and guide to measure its effectiveness.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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 will continue its partnership with Indiana State University and Purdue University.

12. **Who should be main lead of this deliverable?**
    a. IECC Director in coordination with Indiana State University and Purdue University.

13. **What are the expected challenges to completing this deliverable?**
    a. Ensuring the use of the Scorecard is more well-rounded and is a tool for utilizing more of the state's cybersecurity resources.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Initiate next phase of the Scorecard with IECC partner to complete deliverable | Cybersecurity Program Director | 100 | August 2021 | |
| Review Scorecard | Cybersecurity Program Director with Purdue University and Indiana State University | 50 | November 2021 | |
| Draft Changes/Updates to the Scorecard | Cybersecurity Program Director and Program Communications Manager with Purdue University and Indiana State University | 0 | December 2021 | |
| Develop implementation plan | Cybersecurity Program Director and Program Communications Manager | 0 | January 2022 | |
| Identify pilot group | State and Local Government Committee | 0 | January 2022 | |
| Pilot Group complete Scorecard 2.0 | Pilot Group | 0 | June 2022 | |
| Take survey on product | Cybersecurity Program Director | 0 | August 2022 | |
| Make any additional edits based on the pilot group's feedback | Cybersecurity Program Director and Program Communications Manager with Purdue University and Indiana State University | | September 2022 | |
| Develop updated implementation plan for mass public | Cybersecurity Program Director and Program Communications Manager | 0 | September 2022 | |

| | | | | |
|---|---|---|---|---|
| Execute implementation plan for launch of Scorecard 2.0 to public | IECC partners | 0 | October 2022 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 1.5 FTE | N/A | Cybersecurity and business | State of Indiana | IECC Partner | |

**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 |
|---|---|---|---|---|---|---|
| No Response | | | | | | |

## 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 with an updated 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 are the estimated costs associated with that risk reduction?**

a. Scorecard 2.0 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 IECC would have one less resource to share with emergency managers help maintain a higher level of cybersecurity preparedness; one less tool that can be used to measure Indiana's overall 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 2.0 is an output success. Having 90 percent of all sentinel sample complete the Scorecard 2.0.

**21. 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

**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?**

☐No ☒ Yes

a. As of August 2021, according to the National Conference of State Legislators (NCSL), 28 states have created a statewide cybersecurity task force, commission or advisory council or similar group. But no other state has 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?**

☒No ☐ Yes

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

a. It will require someone to have the ability to review and update it as necessary.

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

a. All committees and working groups will be contacted with the Scorecard 2.0

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes

## 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)?**

☐No ☒ 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 Indiana State University and Purdue University, will develop a Scorecard 2.0 with a Level Up Guide to improve cybersecurity posture by January 2022.

*Type:* ☒ Output ☐ Outcome

☒ 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 pilot Indiana's Cybersecurity Scorecard 2.0 with Level Up Guide with local governments by July 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

**Objective 3:** IECC will relaunch Indiana's Cybersecurity Scorecard 2.0 with Level Up Guide to the public by December 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:
# Indiana State of Cyber Report (2017-2021)

# Deliverable: Indiana State of Cyber Report (2017-2021)

## *General Information*

1. **What is the deliverable?**
   a. Indiana Cyber Success Report (2017-2021)

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?**
   ☐ 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 compilation of Cyber Accomplishments will illustrate and provide definition to the success achieved in Indiana with cybersecurity within the IECC and outside the IECC.

6. **What metric or measurement will be used to define success?**
   a. Presentation of successful projects and deliverables both within IECC and its members and entities outside of the Council in public and private sector.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. State, local government, K-12, higher education, and small/medium businesses

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. Not at this time.

## Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All the other committees will be contributing their deliverable updates and strategic plans.

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 state agencies on the IECC will contribute as the are able and the rest of the report will be based on what outside partners (public, private, academia).

12. **Who should be main lead of this deliverable?**
    a. Indiana State Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. It is a volunteer council and with so many things that are priority and a lack of time and resources may also hinder the completion of this deliverable.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Collect/Feature Cyber Accomplishments from IECC members/state agencies and public/private sectors | IECC | 100% | September 2021 | |
| Draft outline | Cybersecurity Program Director | | September 2021 | |
| Draft content | Cybersecurity Program Director | | October 2021 | |
| Layout with graphic designer | Cybersecurity Program Director, IN.gov | | October 2021 | |
| Edit content | IECC project support staff from IOT/IDHS | | October 2021 | |
| Get approval from IDHS/IOT | IDHS Executive Director Cox and Tracy Barnes | | October 2021 | |
| Finalize report | IECC project support staff from IOT/IDHS | | October 2021 | |
| Present report to Governor | IECC Chair Cox and Voting members | | October 29, 2021 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 2 FTE | 1 FTE | Communications | IECC Staff | N/A | |

**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 |
|---|---|---|---|---|---|---|
| No Response | | | | | | |
| | | | | | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. This deliverable provides examples of Indiana's presence as a cybersecurity leader among states in cybersecurity governance, programming, and public awareness/education.

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

a. By continuing to educate and inform Hoosiers about cybersecurity, the knowledge gained by the general public, state and local government, education and the public/private sectors helps mitigate the potential for cyber incidents and cyberattacks, including those involving identity theft and other forms of cybercrime.
b. In the absence of a continued communications campaign – in which the public is informed and encouraged about remaining vigilant as it regards all aspects of cybersecurity and taking a personal responsibility for their part of cyberspace – not having a scorecard could create a higher likelihood that cyber incidents and cyberattacks will occur at a rate that grows, in terms of the severity of what is lost financially, as well as the protection of our own personal identifying information.

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

a. An opportunity is missed to educate and inform Hoosiers about cybersecurity.

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

a. The opportunity to inform Hoosiers regarding the continued progress being achieved in Indiana with cybersecurity.

**21. 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

**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?**

☒No ☐ Yes

## Other Implementation Factors

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

a. Not enough staff or key reviewers not making needed edits on time.

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

☒No ☐ Yes

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

a. IECC staff time to update/collect additional case studies.

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

a. IECC members

**27. Can this deliverable be used by other sectors?**

☒No ☐ Yes,

## Communications

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

a. IECC Members, small/medium small business, state and local government, K-12 and Higher Education

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

☐No ☒ Yes

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

a. Potential to highlight selected case studies as part of the Indiana Cybersecurity Hub website, Cyber Hub Blog and "Days of Our Cyber Lives" podcast with the Treasurer of State, Indiana Bond Bank and IECC.

## *Evaluation Methodology*

**Objective 1**: The Indiana Executive Council on Cybersecurity will develop a report to address the status and successes of the IECC as well as Indiana organizations by October 29, 2021.

*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 2021 Strategic Plan

# Deliverable: IECC 2021 Strategic Plan

## *General Information*

1. **What is the deliverable?**
   a. IECC 2021 Strategic Plan

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.**
   ☒ 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. 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?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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. 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. 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. IOT, IDHS

12. **Who should be main lead of this deliverable?**
    a. State of Indiana Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. It is a volunteer council and with so many things that are priority and a lack of time and resources may also hinder the completion of this deliverable.

## *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Determine what the Framework Document will contain | Program Director, Program Manager | 100% | April 2021 | |
| Develop draft Table of Contents | Program Manager | 100% | April 2021 | |
| Review draft TOC | Program Director, Program Manager | 100% | September 2021 | |
| Develop list of subtopics | Program Director, Program Manager | 100% | March – April 2021 | |
| Begin documenting topics and subtopics | Program Manager | 100% | April 2021 | |
| Determine document design | Program Director, Program Manager | 100% | September 2021 | |
| Complete Draft | Program Manager | 100% | September 2021 | |
| Final Draft approval | Program Director | 100% | October 2021 | |
| Strategic Resource WG approval process | Program Manager | 100% | September 2021 | |
| Complete documentation and Final Review | Program Director | 100% | October 2021 | |
| Integrate document into final report | Program Director, Program Manager | 100% | October 2021 | |

## Resources and Budget

**15. Will staff be required to complete this deliverable?**

☐No ☒ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| 3 FTE | | | State of Indiana – IOT/IDHS | | |

**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 |
|---|---|---|---|---|---|---|
| Technical Editors | Proofreading | $0 | $0 | State of Indiana IOT/IDHS | N/A | |
| Development of graphic design lay out | Design | N/A | N/A | State of Indiana IOT/IDHS | | |

## Benefits and Risks

**17. What is the greatest benefit of this deliverable?**

a. Providing supporting documentation of how the Council was planned, established, and governed in addition to addressing what the Council has accomplished since it's first strategic plan in 2018. Sharing a repeatable framework for other organizations and states to leverage.

**18. How will this deliverable reduce the cybersecurity risk or impact? What are 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 and Strategic Resource Working Group approval in October 2021. The final to the Governor in late October.

**21. 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. Many states now have cybersecurity strategic plans. Indiana, however, is still the leading state of the having the most comprehensive, in-depth 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?**

☐No ☒ Yes

a. Of the states that do not have cybersecurity efforts to the degree of Indiana, they often struggle with public/private partnerships as well as state-agency fighting. These are things we do not experience in Indiana around the cybersecurity strategy.

## 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?**

☒No ☐ Yes

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

a. Maintaining the current structure of the IECC, as it regards the responsibilities of the Cybersecurity Program Director and the collaboration by/between all members of the Council and its leadership.

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

a. State of Indiana Cybersecurity Program Director

**27. Can this deliverable be used by other sectors?**

☐No ☒ Yes,

a. All sectors

## Communications

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

a. IECC, State and Local Government, Public and Private Sector, General Public

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

☐No ☒ Yes

a. It will be posted on the Indiana Cybersecurity Hub website in October 2021.

**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 a 2021 Strategic Plan for the Council by October 29, 2021.

*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: Outreach to Underrepresented Sectors

# Deliverable: Outreach to Underrepresented Sectors

## *General Information*

1. **What is the deliverable?**
   a. To develop an outreach and communications strategy for industrials that are not represented on the council. The ongoing communications strategy will help ensure the council is informed of cyber concerns occurring within these industries and that these industries are aware of the activities and deliverables of the council.

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?**
   ☐ 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. Increased awareness within the council of cyber challenges or concerns within the unrepresented industries. Increase awareness within the industries of activities and deliverables of the council.

6. **What metric or measurement will be used to define success?**
   a. The establishment of primary contacts for each industry and regular meetings to facilitate knowledge sharing between industry and the council.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. The strategic resources working group and the unrepresented industries.

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

## 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. Industry Groups of the unrepresented industries

12. **Who should be main lead of this deliverable?**
    a. The strategic resources working group.

13. **What are the expected challenges to completing this deliverable?**
    a. Establishing the right contacts within each of the unrepresented industries

# *Implementation Plan*

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

## Tactic Timeline

| Tactic | Owner | % Complete | Deadline | Notes |
|---|---|---|---|---|
| Develop list of unrepresented industries | Strategic Resources Committee | 0 | 03/2022 | |
| Identify organizations and primary contacts for each industry | Strategic Resources Committee | 0 | 17/2022 | |

| | | | | |
|---|---|---|---|---|
| Make preliminary introductions to each industry | Strategic Resources Committee | 0 | 12/2022 | |
| Establish regular communication cadence for each industry | Strategic Resources Committee | 0 | 03/2023 | |

## Resources and Budget (Please add rows as needed)

**15. Will staff be required to complete this deliverable?**

☒No ☐ Yes

| Estimated Initial FTE | Estimated Continued FTE | Skillset/Role | Primary Source of Funding | Alternate Source of Funding | Notes |
|---|---|---|---|---|---|
| None | None | | | | |

**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. Providing a communications conduit for unrepresented industries

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

a. By establishing processes to share resources available to Indiana industries that could benefit from the work being performed by the council.

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

a. Increased cyber risks to the unrepresented sectors due to not leveraging the state resources available to them.

**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 by providing the unrepresented industries with the tools and resources to better mitigate cyber risks.

**21. 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

**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?**
☒No ☐ 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?**
☒No ☐ Yes

**25. What will it take to support this deliverable if it requires ongoing sustainability?**
a. Not ongoing

**26. Who has the committee/working group contacted regarding implementing this deliverable?**
a. None

**27. Can this deliverable be used by other sectors?**
☒No ☐ Yes

## Communications

**28. Once completed, which stakeholders need to be informed about the deliverable?**
a. All IECC members

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

**30. What are other public relations and/or marketing considerations to be noted?**
a. As we gather resources and deliverables that will be helpful to other industries, it would be prudent to update the website as well.

## *Evaluation Methodology*

**Objective 1:** With key partners, identify cybersecurity awareness needs in additional Indiana industries (manufacturing, transportation, small business, and agriculture) by December 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

**Objective 2:** Provide industry contacts with education materials and set up a regular communication cadence for each industry by March 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

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 1.0
- Policy Research Report 1.0

# Indiana Scorecard 1.0


**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.

# Policy Research Report 1.0

# An Analysis of Cybersecurity Legislation and Policy Creation on the State Level


| Adam Alexander | Paul Graham | Eric Jackson | Bryant Johnson | Tania Williams |
|---|---|---|---|---|
| aha0007@uah.edu | pag0006@uah.edu | eaj0010@uah.edu | bej0003@uah.edu | 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.

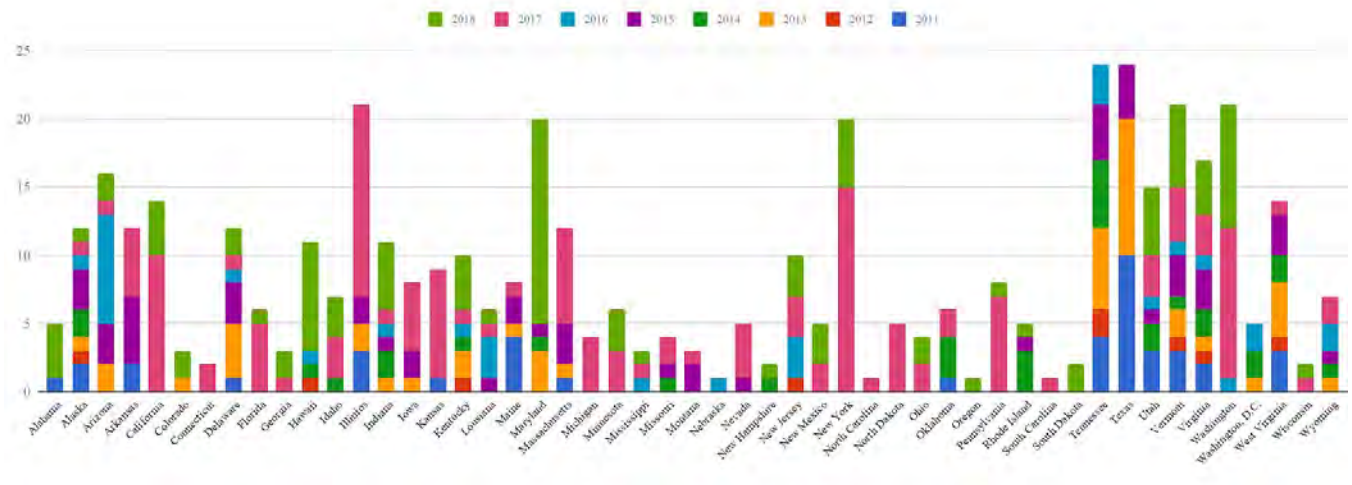



**Figure 1.** The quantity of policies developed by each state per year between 2011 and 2018.

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.

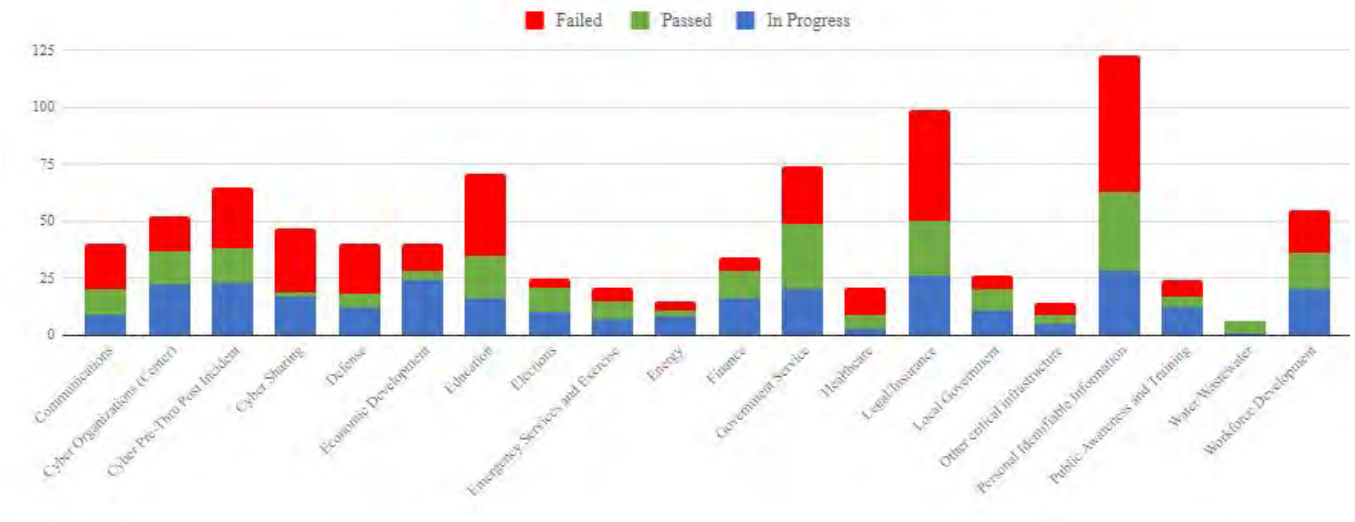



**Figure 2.** The quantity of each policy type surveyed that is either still in process, was passed into law, or was failed for any reason.

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

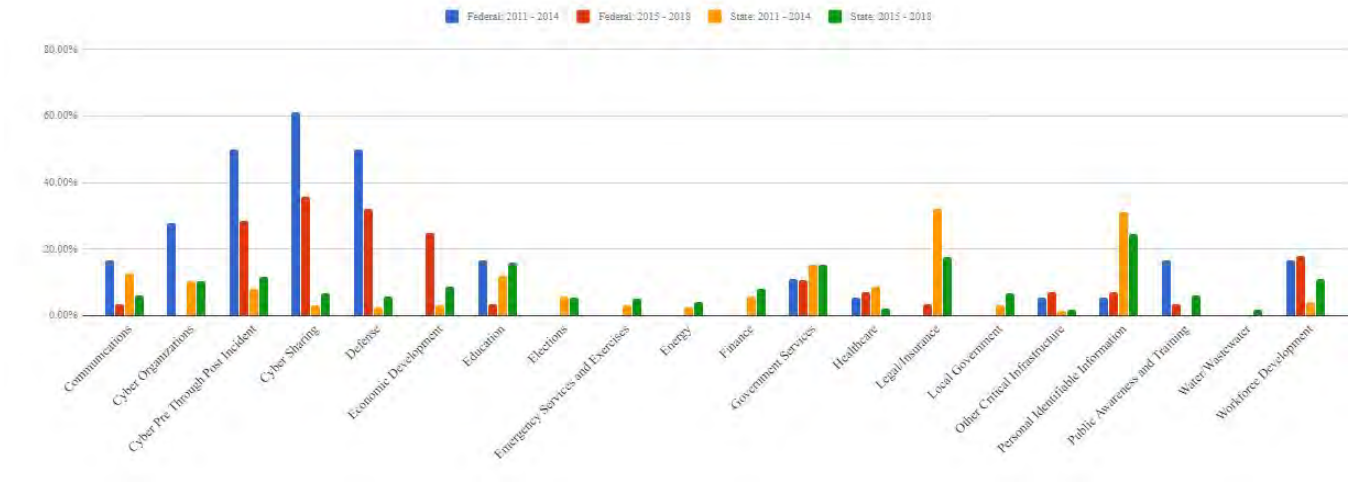



**Figure 3.** The percentage of state and federal policies introduced in 4 year periods (2011-2014, and 2015-18) that deal each surveyed category.

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.

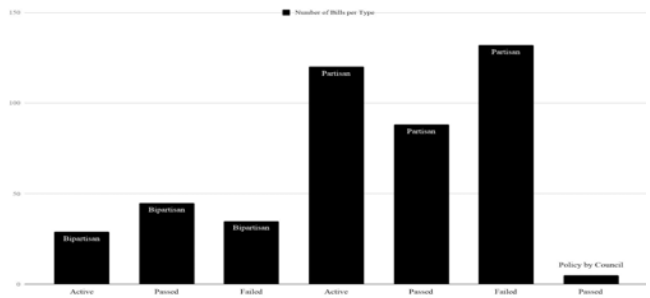



**Figure 4.** Success of state level bipartisan legislation attempts as opposed to partisan legislation attempts.

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 E

## IECC Membership and Leadership List 2018-2021

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** | **Designee 1** | **Title** | **Designee 2** | **Title** |
| John Hammond | State of Indiana | Governor's Office | Senior Operations Director | Micah Vincent | OMB Director | | |
| Bryan Langley | State of Indiana | Indiana Department of Homeland Security | Executive Director | Jordan Bolden | Chief of Staff | | |
| Dewand Neely | State of Indiana | Indiana Office of Technology | CIO | Bryan Sacks | CISO | | |
| Douglas Carter | State of Indiana | Indiana State Police | Superintendent | Larry Turner | Lt. Col, Office of Superintendent | Chuck Cohen | Commander, Intelligence and Investigative Technologies |
| MG Courtney Carr | State of Indiana | Indiana National Guard | Adjutant General | Tim Winslow | COL USARMY NG INARNG | Col. Jeffrey Hackett | INNG Cyber Operations |
| Connie Lawson | State of Indiana | Secretary of State | Secretary of State | Brandon Clifton | Deputy Chief of Staff | | |
| Jim Huston | State of Indiana | Indiana Utility Regulatory Commission | Chair | Sarah Freeman | Commissioner | | |
| Teresa Lubbers | State of Indiana | Indiana Commission for Higher Education | Commissioner | Michael Hawryluk | Chief Technolgoy Officer | | |
| Adam Krupp | State of Indiana | Indiana Department of Revenue | Commissioner | Tony Chu | CISO | | |
| Jim Schellinger | State of Indiana | Indiana Economic Development Corporation | Secretary of Commerce | David Roberts | VP, Chief Innovation Officer | Mark Wasky | Policy Director and Counsel, Policy |
| Brad Wheeler | State of Indiana | Indiana University | CIO | Mark Bruhn | Associate VP of Public Safety and Institutional Assurance | | |
| Curtis Hill | State of Indiana | Attorney General | Attorney General | Douglas Swetnam | Section Chief of Data Privacy and Identity Theft Unit | | |
| Gerry McCartney | State of Indiana | Purdue University | CIO | Greg Hedrick | CISO | Rob Stanfield | Director, Identity Access Management |
| Tracy Barnes | State of Indiana | Lt. Governor's Office - CTASC Representative | Chief of Staff | Ryan Heater | Policy Director | Rebecca Kasper | Special counselor |
| Fred Payne | State of Indiana | Indiana Department of Workforce Development | Commissioner | Steve Elliot | Executive Director | | |
| Danielle Chrysler | State of Indiana | Indiana Office of Defense Development | Director | Ryan Metzing | Ice Miller | | |
| Stephanie Yager | Local Government | Indiana Association of County Commissioners | Executive Director | Mike Yoder | President, Elkhart County | | |
| Rhonda Cook | Local Government | Accelerate Indiana Municipalities (AIM) | Executive Director | Matthew Greller | Executive Director & CEO | | |
| Mark A. Lantzy | Healthcare | IU Health | CIO | Mitchell Parker | CISO | | |
| Joni K. Hart | Communications | Indiana Cable Telecommunications Association | Executive Director | Dan Solero | VP, ATT | | |
| Owen LaChat | Financial Services | MutualBank | Information Security Officer | Sharon Ferguson | Information Security Officer and Chief Risk Officer | | |
| Stephen A. Key | Public Interest - Media | Hoosier State Press Association | Executive Director | Robert Dittmer | REDCOM Public Relations Consulting, Principal | | |
| Ronald W. Pelletier | Cybersecurity/IS | Ponderance | Founding Partner | Landon Lewis | Director | Dennis Porter | COO |
| John Lucas | Water /Wastewater | Citizens | Vice President, IT | Jon F. Weirick | Fort Wayne Utilities, Senior Program Manager | | |
| Mark T. Maassel | Energy | Indiana Energy Association | President | Robert I. Richhart | Hoosier Energy, Vice President, Management Services | Walter Grudzinski | Vectren Corporation, Director, Information Security and Business Continuity |
| David Ehinger | Defense Industrial Base | Rolls Royce | Business Manager for IT Security | Brad Swearington | Rolls Royce | Mary Kate Frazier | Rolls Royce |
| John Davidson | FBI | FBI - Indianapolis Field Office | Supervisory Special Agent | Michael Alford | Supervisory Special Agent | | |
| Paul Dvorak | US DHS | Secret Service | Special Agent in Charge | | | | |
| Tony Enriquez | US DHS | US DHS | Cyber Security Advisor | | | | |

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 |
| JJ Thompson | Rook Security | CEO |

Indiana Executive Council on Cybersecurity -
Membership as of Last Official IECC Vote on January 2018

| | | |
|---|---|---|
| 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 |
| David Greer | Project Lead The Way | Senior Vice President and Chief Program Officer |

Indiana Executive Council on Cybersecurity -
Membership as of Last Official IECC Vote on January 2018

| | | |
|---|---|---|
| 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 |
| Diana Williams | Project Brilliant | Director |

Indiana Executive Council on Cybersecurity -
Membership as of Last Official IECC Vote on January 2018

| | | |
|---|---|---|
| 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

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

# 2019 Council Advisory Membership - For Vote

**FROM:** **Chetrice Mosley, IECC Cybersecurity Program Director**

**TO:** **IECC Voting Members**

**DATE:** **Friday, January 11, 2019**

**NOTE:** These Advisory members marked with an ***asterisk**** will become members as long as all application requirements are met within 30 days of being voted upon.

| Last Name | First Name | Organization | Organizational Title | Member Type: Advisory/ Advisory* |
|---|---|---|---|---|
| Aikman | J. Kurt | Miso Energy | Manager | Advisory |
| Allam | Sandeep | St. Logics | Owner | Advisory* |
| Alley | Mike | Business Resiliency Alliance of Indiana | President | Advisory |
| Babione | John | Wooden McLaughlin | Partner | Advisory* |
| Bagga | Jay | Ball State University | Co-Director, State of Indiana Voting Systems Technical Oversight Program (VSTOP), Professor of Computer Science | Advisory |
| Bailey | Gerry | iLab | Managing Director, North America | Advisory |

| | | | | |
|---|---|---|---|---|
| Bailey | George | Purdue Healthcare Advisors | Security Senior Advisor | Advisory* |
| Baltzell | Paul | Indiana Economic Development Corporation | VP of Information Technology Solutions | Advisory |
| Banta | Rich | Lifeline Datacenters | Partner | Advisory |
| Barefoot | Jonathon | Ivy Tech | Executive Director of Statewide Safety and Security | Advisory |
| Beard | Amy | Indiana Department of Insurance | General Counsel | Advisory |
| Beckman | Joseph | Purdue Healthcare Advisors | Managing Advisor - Security | Advisory* |
| Berry | Scott | Indiana Municipal Power Agency | Manager, Environmental & NERC Compliance | Advisory |
| Berry | Tim | Crowe Horwath | Managing Director/Municipal Advisory Services | Advisory |
| Berry-Tayman | Lisa | Cyber Scout Solutions | Senior Manager, Privacy and Information Guidance | Advisory |
| Berube | Steve | Citizens Energy Group | Manager of Water System Control and Planning | Advisory |
| Bonnet | Jerry | Indiana Secretary of State | General Council | Advisory |
| Bowers | Scott | Indiana Electric Coops | Vice President of Government Relations | Advisory |
| Braidich | Richard | RCR Technology | Chief Information Security Officer | Advisory |
| Britt | Luke | Indiana Office of Public Counselors | Public Access Counselor | Advisory |
| Brown | Allen | Midwest Natural Gas | Director | Advisory |
| Bruhn | Mark | Indiana University | REN-ISAC (need new title) | Advisory |
| Burker | Cody | Cummins, Inc. | | Advisory* |
| Bush | Ron | Ron Bush Consulting | Consultant | Advisory |
| Bushar | Ron | Mandiant | Director | Advisory |
| Butler | Jacob | Parkview Health | Information Security and Compliance Specialist | Advisory |
| Byers | Bryan | Ball State University VSTOP | VSTOP Team Member | Advisory* |
| Calarco | Daniel | Indiana University | Chief of Staff | Advisory |
| Campbell | Jan | Leeuw Oberlies & Campbell, P.C. | Law Partner | Advisory |

| | | | | |
|---|---|---|---|---|
| Campbell | Cliff | Campbell Consulting | President | Advisory |
| Caristi | Dom | Ball State University | Professor of Telecommunications | Advisory |
| Carter | Chris | Indiana State Police | Sergeant, Criminal Investigation | Advisory |
| Carter | Benjamin | Indiana Department of Education | Director of Workforce and Innovation | Advisory |
| Castir (Castor?) | (Tory?) Joan Victoria | IU Health | Senior VP, Government Affairs | Advisory* |
| Chu | Tony | Indiana Department of Revenue | Chief Information Security Officer | Advisory |
| Clark | Ken | City of Indianapolis | Chief Information Officer | Advisory* |
| Clifton | Brandon | Indiana Secretary of State | Deputy Secretary and Chief of Staff | Advisory |
| Cloud | Matthew | Ivy Tech | Project Director - TAACCCT Grant School of IT | Advisory |
| Cohen | Chuck | Indiana State Police | Captain, Criminal Investigation | Advisory |
| Collins | Chris | Indiana InfraGard/KAR Auction Services | President, Enterprise Security Process Manager | Advisory |
| Connell | Chad | Miso Energy | Manager | Advisory |
| Cook | Rhonda | Accelerate Indiana Municipalities | Deputy Director | Advisory |
| Cooper | Seth | Baker Tilly | Project Manager | Advisory |
| Cotterill | Ted | Indiana Management Performance Hub | Chief Privacy Officer and General Counsel | Advisory |
| Cudby | Joe | MXL Consulting | CEO | Advisory |
| Day | David R. | Sallie Mae | Sr. Manager, Identity and Access Management | Advisory |
| Dayhoff-Dwyer | Kathy | Indiana Department of Homeland Security | District Coordinator Liaison | Advisory* |
| De Medeiros | Jennifer | The AES Corporation, US/Indianapolis Power & Light (IPL) | Manager | Advisory |
| Deckard | Gary | Atterbury-Muscatatuck Center | Chief, Technology Division | Advisory |
| Dedon | Jody | Indianapolis Woman in Tech | Executive Director | Advisory* |

| | | | | |
|---|---|---|---|---|
| Dietz | J. Eric | Purdue University | Professor, CIT | Advisory |
| Dignin | Kelly | Integrated Public Safety Commission | Executive Director | Advisory* |
| Dimon | Philip | Health and Hospital Corp | Security Analyst | Advisory* |
| Dingman | Stephanie | Aon PLC | Manager | Advisory |
| Dittmer | Robert | Red Comm Public Relations Consulting | President | Advisory |
| Dlug | Beth | Allen County Election Board | Elections Director | Advisory |
| Donahue | Matthew | LexisNexis Risk Solutions | Director | Advisory |
| Driskell | Debbie | Indiana Township Association | Executive Director | Advisory |
| Ehrenberg | Jim | Indiana Office of Technology | General Counsel | Advisory |
| Eilenberg | Kristin | Lodestone Logic | Founder, CEO | Advisory* |
| Ellis | Greg | Indiana Chamber of Commerce | VP | Advisory |
| Etchison | Matthew | Ivy Tech | VP of Information Technology | Advisory |
| Fahey | Sean | GCR | Elections and Campaign Finance Director | Advisory |
| Fairmouth | Greg | Scofes & Associates Consulting Inc. | Partner | Advisory |
| Ferdon | Mary | City of Columbus | Executive Director Admin, Community Development | Advisory |
| Ferguson | Sharon | MutualBank | Chief Risk Officer, Information Security Officer | Advisory |
| Fite | Tom | Indiana Department of Financial Institutions | Director | Advisory |
| Ford | Russsell | Qumulus Solutions, LLC | President/COO | Advisory* |
| Foreman | Jaimie | City of Carmel Water, INWARN | Drinking Water Regulatory Compliance Administrator | Advisory |
| Frank | Michael | Anderson University | Director of Center for Public Service, Professor | Advisory |
| Fredland | Valita | Indiana Health Information Exchange | Vice President - General Counsel and Privacy Officer | Advisory |

| | | | | |
|---|---|---|---|---|
| Freeman | Sarah | Indiana Utility Regulatory Commission | Commissioner, Chairman & Commissioners | Advisory |
| Funk | Michelle | Indiana Utility Regulatory Commission | Sr Utility Analyst | Advisory |
| Garcia | Carlos | IU Emergency Management | Director, Emergency Management & Continuity | Advisory |
| George | Cornelius | Rook Security | Strategic Business Relationship | Advisory* |
| Giles | Clark | City of Indianapolis | CTO | Advisory* |
| Gilson | Katie | Governor's Office | Executive Assistant To Chief of Staff | Advisory* |
| Glover | Patrick | Indiana Secretary of State | Assistant Director of IT | Advisory |
| Goldman | Jim | Salesforce | VP Security Governance, Risk Management, Compliance | Advisory |
| Goldsmith | Reid | Indianapolis International Airport | Sr Director Information Technology | Advisory* |
| Gonzales | Jose | La Voz | Vice President | Advisory |
| Gonzalez | Armando | Enterprise Integration Corp | VP, Mission Services | Advisory* |
| Goodwin | Travis | Indiana Department of Environmental Management | Senior Environmental Manager, Security in Counter Terrorism Coordinator | Advisory |
| Gordon | James | Indiana National Guard | INNG | Advisory |
| Greene | John | New Lisbon Telephone Company | CEO and General Manager | Advisory |
| Greer | David | Project Lead The Way, Inc. | Sr VP and Chief Program Officer | Advisory |
| Grudzinski | Walter | Vectren Corporation | Director of Information and Business Continuity | Advisory |

| | | | | |
|---|---|---|---|---|
| Guarente | Tom | FireEye | Vice President, External Affairs | Advisory* |
| Hackett | Jeffrey (Col) | Indiana National Guard | Director of Operations | Advisory |
| Hadley | Ryan | Indiana Utility Regulatory Commission | Deputy Director, Legislative and External Affairs | Advisory* |
| Haley | James | City of Fort Wayne | Chief Information Officer | Advisory |
| Hart | Joni K. | Broadband Innovation Group | Executive Director | Advisory |
| Hawryluk | Michael | Indiana Commission for Higher Education | Chief Technology Officer, Finance-IT | Advisory |
| Herzog | Laura | Hendricks County | Elections Supervisor | Advisory |
| Hirsch | Greg | Vincennes University | Associate Professor | Advisory* |
| Hochstetler | Jay | Qumulus | CISO | Advisory* |
| Hoff | Ryan | AIC | Dir of Gov't Affairs/General Counsel | Advisory |
| Hosick | David | Indiana Department of Homeland Security | Communications Director | Advisory* |
| Howell | Michele | Aon Risk Services Central | Vice President, Business Development | Advisory* |
| Huber | Michael | Indianapolis Chamber of Commerce | President, CEO | Advisory* |
| Hughes | Brandi | IODD | Director of Operations | Advisory* |
| Ira | Adam | Kightlinger and Gray | Attorney | Advisory* |
| Jirik | Jiri | Ivy Tech | Cyber Instructor Evansville | Advisory* |
| Johnston | Kathleen | Media Freelancer | Journalist | Advisory |
| Justice | Connie (Dr.) | IUPUI | Professor | Advisory |
| Keller | John (Dr.) | Indiana Department of Education | Chief Information Officer, IT | Advisory |
| Kibry | Manikancesh | Ball State University VSTOP | VSTOP Team Member | Advisory* |
| King | Brad | Indiana Election Commission | Election Division Co-Director | Advisory |
| Kochevar | Matthew | Secretary of State, Election Division | Attorney | Advisory* |
| Kokonas | Erik | Rook Security | VP, Marketing and Customer Acquisition | Advisory* |

| | | | | |
|---|---|---|---|---|
| Korty | Andrew | Indiana University | Information Security Officer | Advisory |
| Kroft | Kent | Tippecanoe County | CIO | Advisory* |
| Lacy | Peter | Indiana Bureau of Motor Vehicles | Commissioner | Advisory |
| Langelier | Mike | Techpoint | President | Advisory |
| Lederman | Jaci | Vincennes University | Department Chair | Advisory* |
| Lee | Jamie | Wabash National Corporation | VP of IT, CIO | Advisory |
| Lefever | David | Mako Group | CEO | Advisory* |
| Lewis | Landon | Pondurance | Chief Executive Officer | Advisory |
| Linder | Jared | FSSA | CIO | Advisory* |
| Lodin | Steve | Sallie Mae | Sr Director, Cyber Security Operations | Advisory* |
| Loepker | Mark | INsURE | Director | Advisory |
| Lohrentz | John | Munster Police Department | Intelligence Analyst , Computer Forensics | Advisory |
| Lowmiller | Jason | Lowmiller Consulting Group | Cybersecurity Consultant, Trainer | Advisory* |
| Lubsen | Graig | Indiana Office of Technology | Director of Communications | Advisory |
| Lyle | George | Purdue University | IT Security Risk Analyst | Advisory |
| Mabry | Kevin | Sentree Systems, Corp. | Owner | Advisory |
| Mackey | William | Indiana State University | Assistant Professor | Advisory |
| MacLellan | Thomas | Symantec | Government Affairs | Advisory |
| Maddox | James | CenturyLink | Director - SLED KY/IN/MI/OH | Advisory* |
| Martin | Jessica | Ball State University VSTOP | VSTOP Manager | Advisory* |
| Mathis | Dan | DWD | Deputy General Counsel | Advisory* |
| McAninch | Paul | IU Health | Director Information Security & Compliance | Advisory |
| McCullough | Cliff | Family and Social Services Administration | Chief Privacy Officer | Advisory |
| McGinnis | Brian | Barnes & Thornburg LLP | Partner | Advisory |
| McGraw | Michael | Secure Works | Security Systems Advisor | Advisory* |
| McGuinness | Joe | Indiana Department of Transportation | Commissioner | Advisory* |

| | | | | |
|---|---|---|---|---|
| Merkner | Karl | United Federal Credit Union | Security Administrator | Advisory* |
| Mertens | Chris | Hamilton County | Director of IT | Advisory |
| Metzger | Kimberly | Ice Miller | Partner | Advisory |
| Metzinger | Ryan | Ice Miller | Director of Aerospace & Defense Services Director | Advisory |
| Milford | Kim | Indiana University | Lead REN-ISAC | Advisory |
| Miller | Scott | Citizens Energy Group | Cyber Security Manager | Advisory |
| Moorhead | Philip | Ivy Tech | Program Director | Advisory* |
| Needham | C. Nicole | Indiana Office of Technology | Security Awareness Manager | Advisory |
| Nevers | Frank | Federal Home Loan Bank of Indianapolis | Information Security Program Manager | Advisory |
| Norris | Matthew | Krieg DeVault | DISH Network, Satellite Broadcasting and Communications Association | Advisory |
| Nussmeyer | Angela | Indiana Election Commission | Election Division Co-Director | Advisory |
| O'Connor | Dan | City of South Bend | CTO, Innovation and Technology | Advisory* |
| Odum | Matt | Briljent | President | Advisory |
| O'Hara | Brian | InfraGard | Past President of Infragard | Advisory |
| Ortiz | Jason | Pondurance | Senior Software Engineer | Advisory |
| Owen | Dan | Elevate | Consultant | Advisory |
| Parker | Mitchell | IU Health | Executive Director, Information Systems | Advisory |
| Partlow | Stan | American Electric Power (AEP)/Indiana Michigan Power (I&M) | VP & Chief Security Officer | Advisory |
| Phelps | Tasha | Phelco Technologies, Inc. | President | Advisory |
| Phelps | Jay | Bartholomew County | Clerk | Advisory |
| Pirau | Ron | Archdiocese of Indianapolis | CIO | Advisory* |
| Pittman | Chad | Purdue Research Foundation | VP | Advisory |
| Pollitt | Chad | Indiana University | Adjunct Professor of Digital Marketing | Advisory |

| | | | | |
|---|---|---|---|---|
| Pomper | Gale | NetworkNow! | Consultant | Advisory* |
| Porter | Dennis | Pondurance | Director of Operations | Advisory |
| Powell III | Adam | USC Annenberg Center on Communication Leadership and Policy<br>University of Southern California | Director, Washington Programs, and Project Manager, Internet of Things (IoT) Emergency Response Initiative | Advisory* |
| Prostko | Robert | Allegion, plc | Chief Cybersecurity Counsel | Advisory* |
| Putnam | Reid | Gregory & Appel Insurance | Vice President, Commercial Insurance | Advisory* |
| Rapp | Douglas | Cyber Leadership Alliance | President | Advisory |
| Rasmus | Joel | Purdue University (CERIAS) | CERIAS Director | Advisory |
| Ravenna | Leon | KAR Auction Services | Chief Information Security Officer | Advisory |
| Resnick | Dan | Anthem | Information Security Executive Advisor | Advisory* |
| Reuhs | Nicholas | Ice Miller | Partner | Advisory |
| Reuter | Ed | Indiana Statewide 911 Board | Executive Director | Advisory |
| Reynolds | Stephen (Steve) | Ice Miller | Partner | Advisory |
| Richhart | Robert | Hoosier Energy | Vice President | Advisory |
| Riggi | John | American Hospital Association (AHA) | Senior Advisor, Cybersecurity and Risk | Advisory* |
| Ritter | Barry | Indiana Statewide 911 Board | Director | Advisory |
| Roberts | David | Indiana Economic Development Corporation | Vice President, Chief Innovation Officer, Business Development | Advisory |

| | | | | |
|---|---|---|---|---|
| Rockensuess | Brian | Indiana Department of Environmental Management | Chief of Staff | Advisory |
| Roeder | John | Lt. Governor's Office | Special Assistant | Advisory* |
| Rogers | Marcus | Purdue Polytechnic | Department Head | Advisory* |
| Romero | Joseph (Joe) | IU Health | Emergency Preparedness Program Manager | Advisory |
| Ross | Michael | Criminal Justice Institute | Director | Advisory* |
| Rudd | Scott | Lt. Governor's Office | Director of Broadband Opportunities | Advisory* |
| Rupel | Johnathan (CPT) | Raytheon | Cyber Engineer | Advisory* |
| Russell | Bill | Cummins, Inc. | Chief Information Security Officer | Advisory |
| Sacks | Bryan | Indiana Office of Technology | CISO | Advisory |
| Salahieh | Rami Mohamad | Ivy Tech | Assistant Professor for Cyber Security & Information Assurance | Advisory |
| Scarbro Kennedy | Valinda | IBM | Global Academic Programs Director | Advisory* |
| Schenck | Ashley | Indiana Management Performance Hub | Director of Engagement and Analytics | Advisory |
| Schmelz | Pam | Ivy Tech | Department Chair | Advisory* |
| Schroers | Steven | Lake County 911 | I.T. Manager/Local Agency Security Officer | Advisory* |
| Scofes | Steve | Scofes & Associates Consulting Inc. | President | Advisory |
| Scribner | Adam | Indiana University Bloomington | Director of STEM Education Initiatives | Advisory* |
| Searcy | Adam | Effective Computer Solutions | President | Advisory* |
| Shemroske | Kenneth | University of Southern Indiana | Associate Professor of CIS | Advisory* |
| Sigfried-Spellar | Kathryn | Purdue | Assistant Professor | Advisory* |
| Skalon | Dave (LT) | Indiana National Guard | INNG Cyber Mission | Advisory |
| Smith | Roosevelt | Cyborsonar | Founder | Advisory* |
| Stahl | Tad | IN-ISAC / Indiana Intelligence Fusion Center | Director / Deputy Director for Cyber Intelligence | Advisory |

| | | | | |
|---|---|---|---|---|
| Stone | Brad | Indiana Department of Financial Institutions | Director of Information Technology | Advisory |
| Stouder | Kevin | Indiana Department of Financial Institutions | IT Examiner, IT Program Lead | Advisory |
| Sturgeon | Nick | Ernst & Young | Cybersecurity Advisory | Advisory |
| Swearingen | Mark | Hall, Render, Killian, Heath & Lyman, P.C. | Attorney, health information privacy and security | Advisory |
| Swetnam | Douglas | Indiana Office of Attorney General | Section Chief – Data Privacy & Identity Theft Unit | Advisory |
| Taggart | Krista | City of Greenwood | Corporation Counsel | Advisory |
| Taylor | Curtis | Wabash Valley Power Authority (WVPA) | VP, Technical Services | Advisory |
| Templeman | Robert | Crane | Director | Advisory* |
| Thompson | JJ | Rook Security | Owner | Advisory |
| Togashi | Darryl | Ivy Tech | Department Chair, Cyber Security | Advisory |
| Tooley | Cliff (GEN) | NCCO | Director | Advisory |
| Tucek | William | Navient | Director, Cyber Security | Advisory |
| Tucker | Brett | Carnegie Mellon University, SEI, CERT | Technical Manager, Cyber Risk Management | Advisory* |
| Tucker | Jeff | Dept of Workforce Development | Chief Information Officer | Advisory |
| Turner | Larry | Indiana State Police | Lt Colonel, Off Of The Asst Supt | Advisory |
| Tygart | David | Indiana National Guard (INNG), J36 | J36, INNG | Advisory |
| Umberger | Geanie | Purdue University | Associate Dean for Engagement | Advisory |
| Valle | Alejandro | Citizens Energy Group | Senior Legal Counsel | Advisory |

| | | | | |
|---|---|---|---|---|
| Vanderpool | Tom | Indiana Department of Transportation | Emergency Planning & Response Director, Highway Management | Advisory |
| VanZee | Andrew | Indiana Hospital Association | Vice President | Advisory |
| Vare | Todd | Barnes & Thornburg LLP | Partner | Advisory |
| Vespa | Tony | Vespa Group, LLC | Owner | Advisory |
| Vessely | Thomas | Indiana Secretary of State | Director of IT | Advisory |
| Vincent | Julie | IUPUI | Public Relations Lecturer | Advisory |
| Vincent | Micah | Indiana Office of Management & Budget | OMB Director, Governor's Office | Advisory |
| Vitale | Brian | Notre Dame Federal Credit Union | Chief Risk & Compliance Officer | Advisory |
| Walls | Brent | Indiana Department of Corrections | Information Security Manager | Advisory* |
| Warycha | Valerie | Indiana Secretary of State | Communications Director, HAVA | Advisory |
| Wasky | Mark | Indiana Economic Development Corporation | Vice President & Counsel, Government & Community Affairs | Advisory |
| Weber | Jim | Raytheon | Cybersecurity and Specialty Engineering, Dept Manager | Advisory |
| Weirick | Jon F. | City of Ft Wayne | Engineer / Utilities | Advisory |
| Welch | Von | Indiana University | Director, Center for Applied Cybersecurity Research | Advisory |
| Werner | Kyle | Crane | Strategic Director | Advisory |
| Wessler | Martin | Wessler Engineering | CEO | Advisory |
| Wichlinski | Bob | Valparaiso University | Lecturer | Advisory* |
| Williams | Diana | Project Brilliant | Director | Advisory |
| Wilson | Bill | Indiana Sheriff's Association | Jail Services Coordinator | Advisory* |
| Wolfenden | Bradley | Circadence | Director of Academic Partnerships | Advisory* |
| Woods | Jo Angela (Jodie) | Accelerate Indiana Municipalities | General Counsel | Advisory |
| Woolsey | Bill | BMV | Director of Information Security | Advisory* |

| | | | | |
|---|---|---|---|---|
| Wright | Carolyn | Indiana Municipal Power Agency | Vice President | Advisory |
| Wuellner | Mark | Indiana Bond Bank | Executive Director | Advisory* |

# 2020 Indiana Executive Council on Cybersecurity

| Last Name | First Name | Organization | Organizational Title |
|---|---|---|---|
| Aikman | J. Kurt | Miso Energy | Senior Security Advisor |
| Allam | Sandeep | St. Logics | Owner |
| Alley | Mike | Business Resiliency Alliance of Indiana | President |
| Babione | John | Wooden McLaughlin | Partner |
| Backes | Andrea | Vectren / Centerpoint | Manager, Governance, Risk & Compliance |
| Bagga | Jay | Ball State University | Co-Director, State of Indiana Voting Systems Technical Oversight Program (VSTOP), Professor of Computer Science |
| Bailey | George | Purdue Healthcare Advisors | Security Senior Advisor |
| Bailey | Gerry | Corvano | President |
| Baltzell | Paul | Indiana Economic Development Corporation | VP of Information Technology Solutions |
| Banta | Rich | Lifeline Datacenters | Partner |
| Barefoot | Jonathon | Ivy Tech | Executive Director of Statewide Safety and Security |
| Beard | Amy | Indiana Department of Insurance | General Counsel |
| Beckman | Joseph | Purdue Healthcare Advisors | Managing Advisor - Security |
| Berry | Scott | Indiana Municipal Power Agency | Manager, Environmental & NERC Compliance |
| Berry | Tim | Crowe Horwath | Managing Director/Municipal Advisory Services |
| Berry-Tayman | Lisa | Formstack | Privacy and compliance officer |
| Berube | Steve | Citizens Energy Group | Manager of Water System Control and Planning |
| Best | Gerald | Aunalytics | Big Data Expert |
| Bonnet | Jerry | Indiana Secretary of State | General Council |
| Braidich | Richard | RCR Technology | Chief Information Security Officer |
| Britt | Luke | Indiana Office of Public Counselors | Public Access Counselor |

| | | | |
|---|---|---|---|
| Brown | Allen | Midwest Natural Gas | Director |
| Bruhn | Mark | REN-ISAC/ Indiana University | Assessment Engagement Manager |
| Bush | Ron | Ron Bush Consulting | Consultant |
| Bushar | Ron | Mandiant | Director |
| Butler | Jacob | Parkview Health | Information Security and Compliance Specialist |
| Byers | Bryan | Ball State University VSTOP | Co-Director, State of Indiana Voting Systems Technical Oversight Program (VSTOP), Professor of Criminal Justice and Criminology |
| Calarco | Daniel | Indiana University | Chief of Staff |
| Carter | Chris | Indiana State Police | Sergeant, Criminal Investigation |
| Cerny | Kirk | Haystax | Director |
| Chrislip | Chris | EICorp | Senior Cyber Policy Advisor |
| Chu | Tony | Indiana Department of Revenue | Chief Information Security Officer |
| Clark | Ken | City of Indianapolis | Chief Information Officer |
| Clifton | Brandon | Indiana Secretary of State | Deputy Secretary and Chief of Staff |
| Cloud | Matthew | Ivy Tech | Assistant Professor and Department Chair, School of Information Technology |
| Collins | Chris | InfraGard / KAR Auction Services | President, Enterprise Security Process Manager |
| Connell | Chad | Miso Energy | Manager |
| Cooper | Seth | Baker Tilly | Project Manager |

| | | | |
|---|---|---|---|
| Cotterill | Ted | Indiana Management Performance Hub | Chief Privacy Officer and General Counsel |
| Cudby | Joe | Indiana Office of Technology | CTO |
| Day | David R. | Ambassador Solutions | Information Security Consultant |
| Dayhoff-Dwyer | Kathy | Indiana Department of Homeland Security | District Coordinator Liaison |
| Deckard | Gary | Atterbury-Muscatatuck Center | Chief, Technology Division |
| Dedon | Jody | NextLevel Growth | Chief Executive Officer |
| Dietz | J. Eric | Purdue University | Professor, CIT |
| Dignin | Kelly | Integrated Public Safety Commission | Executive Director |
| Dimon | Philip | Health and Hospital Corp | Security Analyst |
| Dingman | Stephanie | Aon PLC | Manager |
| Dittmer | Robert | Red Comm Public Relations Consulting | President |
| Dlug | Beth | Allen County Election Board | Elections Director |
| Donahue | Matthew | LexisNexis Risk Solutions | Director |
| Driskell | Debbie | Indiana Township Association | Executive Director |
| Ehrenberg | Jim | Indiana Office of Technology | General Counsel |
| Ellis | Greg | Indiana Chamber of Commerce | VP |
| Embrey | Nathan | Evansville Water and Sewer | Deputy Director - IT |
| Etchison | Matthew | Ivy Tech | VP of Information Technology |
| Fahey | Sean | GCR | Elections and Campaign Finance Director |
| Fairmouth | Greg | Scofes & Associates Consulting Inc. | Partner |
| Ferdon | Mary | City of Columbus | Executive Director Admin, Community Development |
| Ferguson | Sharon | MutualBank | Senior VP,Chief Risk Officer, Information Security Officer |

| | | | |
|---|---|---|---|
| Fite | Tom | Indiana Department of Financial Institutions | Director |
| Foltz | Jeramy | AT&T | Sr Technical Team Lead |
| Foreman | Jaimie | City of Carmel Water, INWARN | Drinking Water Regulatory Compliance Administrator |
| Frank | Michael | Anderson University | Director of Center for Public Service, Professor |
| Fredland | Valita | Indiana Health Information Exchange | Vice President - General Counsel and Privacy Officer |
| Freeman | Sarah | Indiana Utility Regulatory Commission | Commissioner, Chairman & Commissioners |
| Funk | Michelle | Indiana Utility Regulatory Commission | Sr Utility Analyst |
| Garcia | Carlos | IU Emergency Management | Director, Emergency Management & Continuity |
| Garmon | Joe | Wabash Valley Power Authority (WVPA) | Director of IT Policy and Cybersecurity |
| Giles | Clark | City of Indianapolis | CTO |
| Glover | Patrick | Indiana Secretary of State | Director of Information Security |
| Goldman | Jim | Salesforce | VP Security Governance, Risk Management, Compliance |
| Goldsmith | Reid | Indianapolis International Airport | Sr Director Information Technology |
| Gonzales | Jose | La Voz | Vice President |
| Goodwin | Travis | Indiana Department of Environmental Management | Senior Environmental Manager, Security in Counter Terrorism Coordinator |
| Gordon | James | Indiana National Guard | INNG |
| Greene | John | New Lisbon Telephone Company | CEO and General Manager |
| Greer | David | Project Lead The Way, Inc. | Sr VP and Chief Program Officer |

| | | | |
|---|---|---|---|
| Gregg | John | Accelerate Indiana Municipalities | Grassroots Legislative Advocate |
| Groves | Justin | iLab | IT Security |
| Grudzinski | Walter | PwC | Director and Global Head, Business Continuity and Disaster Recovery |
| Guarente | Tom | FireEye | Vice President, External Affairs & Alliances |
| Hackett | Jeffrey (Col) | Indiana National Guard | External Affairs & Alliances |
| Hadley | Ryan | Indiana Utility Regulatory Commission | External Affairs |
| Haley | James | City of Fort Wayne | Chief Information Officer |
| Harper | Bryan | Indiana State Police | Criminal Investigation |
| Hart | Joni K. | Broadband Innovation Group | Executive Director |
| Hawryluk | Michael | Indiana Commission for Higher Education | Chief Technology Officer, Finance-IT |
| Herzog | Laura | Hendricks County | Elections Supervisor |
| Hirsch | Greg | Vincennes University | Assistant Professor |
| Hochstetler | Jay | Qumulus | CISO |
| Holmes | Evan | Centerpoint/Vectren | Manager, Information Security and Business Continuity |
| Hosick | David | Indiana Department of Homeland Security | Communications Director |
| Howell | Michele | Aon Risk Services Central | Vice President, Business Development |
| Hughes | Brandi | IEDC – Defense | Deputy Director |
| Ira | Adam | Kightlinger and Gray | Attorney |
| Jackson | Craig | IU CACR | Program Director |
| Johnston | Kathleen | Michael I. Arnolt Center for Investigative Journalism, Indiana University | Founding Director |
| Justice | Connie (Dr.) | IUPUI | Professor |
| Keller | John (Dr.) | Indiana Department of Education | Chief Information Officer, IT |
| King | Brad | Indiana Election Commission | Election Division Co-Director |

| | | | |
|---|---|---|---|
| Koressel | Jake | IDOE | Computer Science Specialist |
| Korty | Andrew | Indiana University | Information Security Officer |
| Lacy | Peter | Indiana Bureau of Motor Vehicles | Commissioner |
| Langelier | Mike | Techpoint | President |
| Lederman | Jaci | Vincennes University | Chair<br>Information Technology Department |
| Lee | Jamie | Wabash National Corporation | VP of IT, CIO |
| Lefever | David | Mako Group | CEO |
| Lewis | Landon | Pondurance | Chief Executive Officer |
| Linder | Jared | FSSA | CIO |
| Lodin | Steve | Sallie Mae | Sr Director, Cyber Security Operations |
| Loepker | Mark | INsURE | Director |
| Lohrentz | John | Munster Police Department | Intelligence Analyst , Computer Forensics |
| Lowmiller | Jason | Lowmiller Consulting Group | Owner/Trainer |
| Lubsen | Graig | Indiana Office of Technology | Director of Communications |
| Lyle | George | Purdue University | IT Security Risk Analyst |
| Mabry | Kevin | Sentree Systems, Corp. | Owner |
| Mackey | William | Indiana State University | Assistant Professor |
| MacLellan | Thomas | Symantec | Government Affairs |
| Mathis | Dan | Indiana Office of Technology | Compliance Manger |
| Mays | Lindsey | Indiana Secretary of State | IT Director |
| McCauley | John | Bingham, Greenebaum, and Doll | Partner |
| McCullough | Cliff | Family and Social Services Administration | Chief Privacy Officer |
| McDonald | John | Clear Object | CEO |
| McGinnis | Brian | Barnes & Thornburg LLP | Partner |
| McGraw | Michael | Secure Works | Security Systems Advisor |

| | | | |
|---|---|---|---|
| McGuinness | Joe | Indiana Department of Transportation | Commissioner |
| Meadors | Joe | Gaylor Electric Inc | VP of Information Services |
| Merkner | Karl | United Federal Credit Union | Security Administrator |
| Mertens | Chris | Hamilton County | Director of IT |
| Metzger | Kimberly | Ice Miller | Partner |
| Metzing | Ryan | Ice Miller | Director of Aerospace & Defense Services Director |
| Milford | Kim | Indiana University | Lead REN-ISAC |
| Miller | Scott | Citizens Energy Group | Cyber Security Manager |
| Moorhead | Philip | Ivy Tech | Program Director (RETD). Adjunct Professor |
| Needham | C. Nicole | Indiana Office of Technology | Security Awareness Manager |
| Neely | Dewand | ElevenFifty Academy | CIO |
| Nevers | Frank | Consultant | Senior Information Security Risk Management |
| Nussmeyer | Angela | Indiana Election Commission | Election Division Co-Director |
| Odum | Matt | Briljent | President |
| O'Hara | Brian | National Conference of Insurance Guaranty Funds | CISO |
| Ortiz | Jason | Pondurance | Senior Software Engineer |
| Owen | Dan | Sexton's Creek | Consultant |
| Parker | Mitchell | IU Health | Executive Director, Information Systems |
| Phelps | Jay | Bartholomew County | Clerk |

| | | | |
|---|---|---|---|
| Phelps | Tasha | Phelco Technologies, Inc. | President |
| Pirau | Ron | Archdiocese of Indianapolis | CIO |
| Pittman | Chad | Purdue Research Foundation | VP |
| Pollitt | Chad | Indiana University | Adjunct Professor of Digital Marketing |
| Porter | Dennis | Pondurance | Director of Operations |
| Prostko | Robert | Allegion, plc | Chief Cybersecurity Counsel |
| Putnam | Reid | Gregory & Appel Insurance | Vice President, Commercial Insurance |
| Rapp | Douglas | Cyber Leadership Alliance | President |
| Rasmus | Joel | Purdue University (CERIAS) | CERIAS Director |
| Ravenna | Leon | KAR Auction Services | Chief Information Security Officer |
| Resnick | Dan | Anthem | Information Security Executive Advisor |
| Reuhs | Nicholas | Ice Miller | Partner |
| Reuter | Ed | Indiana Statewide 911 Board | Executive Director |
| Reynolds | Brent | Naval Surface Warfare Center (NSWC) | Chief Scientist (C5ISR, Integration Div.) |
| Reynolds | Stephen | Ice Miller | Partner |
| Richhart | Robert | Hoosier Energy | CTO |
| Roberts | David | Indiana Economic Development Corporation | Vice President, Chief Innovation Officer, Business Development |
| Rockensuess | Brian | Indiana Department of Environmental Management | Chief of Staff |
| Roeder | John | Lt. Governor's Office | Director of Advance Planning |
| Rogers | Marcus | Purdue Polytechnic | Department Head |
| Romero | Joseph (Joe) | IU Health | Emergency Preparedness Program Manager |
| Ross | Michael | Criminal Justice Institute | Division Director |
| Rudd | Scott | Lt. Governor's Office | Director of Broadband Opportunities |

| | | | |
|---|---|---|---|
| Rupel | Johnathan (CPT) | Raytheon | Cyber Engineer |
| Russell | Bill | Cummins, Inc. | Chief Information Security Officer |
| Sacks | Bryan | Indiana Office of Technology | CISO |
| Salahieh | Rami Maximus | Ivy Tech | Program Chair: Cyber Security & Information Assurance, NIISSA Cyber Security Group |
| Scarbro Kennedy | Valinda | IBM | Global Academic Programs Director |
| Schenck | Ashley | Indiana Management Performance Hub | Director of Engagement and Analytics |
| Schmelz | Pam | Ivy Tech | Chair, School of Information Technology |
| Schroers | Steven | Winston and Strawn, LLP | Technical Support Supervisor |
| Scofes | Steve | Scofes & Associates Consulting Inc. | President |
| Scribner | Adam | Indiana University Bloomington | Director of STEM Education Initiatives |
| Shemroske | Kenneth | University of Southern Indiana | Associate Professor of CIS |
| Sigfried-Spellar | Kathryn | Purdue | Assistant Professor |
| Skalon | Dave (LTC) | Indiana National Guard | INNG CIO |
| Stahl | Tad | IN-ISAC / Indiana Intelligence Fusion Center | Director / Deputy Director for Cyber Intelligence |
| Stone | Brad | Indiana Department of Financial Institutions | Director of Information Technology |
| Stouder | Kevin | Indiana Department of Financial Institutions | IT Examiner, IT Program Lead |
| Sturgeon | Nick | IU Health & IU School of Medicine | Director, Information Security |
| Swearingen | Brad | Rolls Royce | Director of Cybersecurity, Defense Products |

| | | | |
|---|---|---|---|
| Swearingen | Mark | Hall, Render, Killian, Heath & Lyman, P.C. | Attorney, health information privacy and security |
| Swetnam | Douglas | Indiana Office of Attorney General | Section Chief – Data Privacy & Identity Theft Unit |
| Swick | Steve | American Electric Power (AEP)/Indiana Michigan Power (I&M) | VP & Chief Security Officer |
| Taggart | Krista | City of Greenwood | Corporation Counsel |
| Taylor | Curtis | Wabash Valley Power Authority (WVPA) | VP, Technical Services |
| Thompson | JJ | Sophos | Sr. Director Managed Threat Response |
| Togashi | Darryl | Ivy Tech | Department Chair, Cyber Security |
| Tucker | Brett | Carnegie Mellon University, SEI, CERT | Technical Manager, Cyber Risk Management |
| Tucker | Jeff | Dept of Workforce Development | Chief Information Officer |
| Turner | Larry | Indiana State Police | Lt Colonel, Off Of The Asst Supt |
| Tygart | David | Indiana National Guard | J36 Defensive Cyber Programs |
| Umberger | Geanie | Purdue University | Associate Dean for Engagement |
| Valle | Alejandro | Citizens Energy Group | Senior Legal Counsel |
| VanZee | Andrew | Indiana Hospital Association | Vice President |
| Vare | Todd | Barnes & Thornburg LLP | Partner |
| Vespa | Tony | Vespa Group, LLC | Owner |
| Vitale | Brian | Notre Dame Federal Credit Union | Chief Risk & Compliance Officer |
| Walls | Brent | Indiana Department of Corrections | Information Security Manager |
| Warycha | Valerie | Indiana Secretary of State | Communications Director, HAVA |
| Wasky | Mark | Indiana Economic Development Corporation | Vice President & Counsel, Government & Community Affairs |
| Weber | Jim | Raytheon | Cybersecurity and Specialty Engineering, Dept Manager |
| Weirick | Jon F. | City of Ft Wayne | Sr. Program Manager of Automation |
| Welch | Von | Indiana University | Director, Center for Applied Cybersecurity Research |
| Werner | Kyle | Crane | Strategic Director |
| Wessler | Martin | Wessler Engineering | CEO |

| | | | |
|---|---|---|---|
| Wichlinski | Bob | Valparaiso University | Lecturer |
| Williams | Diana | Project Brilliant | Director |
| Winslow (BG) | Timothy | Indiana National Guard | |
| Woods | Jo Angela (Jodie) | Accelerate Indiana Municipalities | General Counsel |
| Wright | Carolyn | Indiana Municipal Power Agency | Vice President |
| Wuellner | Mark | Indiana Bond Bank | Executive Director |

2021 Indiana Executive Council on Cybersecurity
Membership List

| Last Name | First Name | IECC Member Type | Organization | Title |
|---|---|---|---|---|
| Adenike O. | Adetola | Contributing | 360 Security United | SOC |
| Aikman | J. Kurt | Advisory | MISO Energy | Senior Security Advisor |
| Akgul | Arif | Advisory | Indiana State University | Assistant Professor - School of Criminology & Security Studies |
| Alby | Kiran | Guest | Anthem, Inc. | Intern |
| Alley | Mike | Advisory | Resilient Strategies, LLC | President |
| Ayers | David | Advisory | Indiana Office of Technology | Program Communications Manager |
| Babione | John | Advisory | Dinsmore & Shohl LLP | Partner |
| Bagga | Jay | Advisory | Ball State University VSTOP | Co-Director, State of Indiana Voting Systems Technical Oversight Program (VSTOP), Professor of Computer Science |
| Bailey | Gerry | Advisory | Corvano LLC | President |
| Bailey | George | Contributing | Purdue University / cyberTAP | Assistant Director, cyberTAP / Professional Services |
| Baldwin | Ashley | Advisory | Indiana Department of Homeland Security | State Exercise Officer |
| Banta | Rich | Advisory | Lifeline Datacenters | Principal & Chief Information Security Officer |
| Barefoot | Jonathon | Advisory | IU Health | Vice President |
| Barnes | Tracy | Voting | Indiana Office of Technology | Chief Information Officer |
| Beard | Amy | Advisory | Indiana Governor's Office | Policy Research |
| Beckman | Joe | Advisory | Purdue Technical Assistance Program | Managing Advisor - Security |
| Berry | Tim | Advisory | Crowe, LLP | Managing Director |
| Berry | Scott | Advisory | Indiana Municipal Power Agency | Compliance Manger |
| Berryman | Glenn | Advisory | Community Health Network | CISO |
| Berry-Tayman | Lisa | Advisory | Formstack | Privacy and Compliance Officer |

| Best | Gerald | Contributing | Astro Logistic Solutions | Managing Director |
|---|---|---|---|---|
| Bonnet | Jerry | Contributing | Indiana Secretary of State | General Council |
| Bowen | Brandon | Contributing | Indiana Utility Regulatory Commission | Senior Utility Analyst |
| Bowers | Scott | Advisory | Hoosier Energy REC | Sr. VP Government and Community Relations |
| Braidich | Richard | Advisory | RCR Technology | Chief Information Security & Privacy Officer |
| Britt | Luke | Advisory | Indiana Office of Public Counselors | Public Access Counselor |
| Broniarcayk | Steve | Non-Voting | US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency | Protective Security Advisor |
| Brown | Allen | Advisory | Midwest Natural Gas | IT Director |
| Browning | Karl | Voting | Purdue University | Vice President, Chief Information Officer |
| Bruhn | Mark | Guest | Indiana University REN-ISAC | Consultant |
| Bush | Ron | Advisory | Ron Bush Consulting, Inc. | President |
| Butler | Jacob | Advisory | Parkview Health | Manager of Enterprise Systems |
| Byers | Bryan | Contributing | Ball State University VSTOP | Co-Director, State of Indiana Voting Systems Technical Oversight Program (VSTOP), Professor of Criminal Justice and Criminology |
| Carroll | Alex | Contributing | Lifeline Datacenters | Principal |
| Carter | Douglas | Voting | Indiana State Police | Superintendent |
| Cerny | Kirk | Contributing | Haystax, A Fishtech Group Company | Senior Director |
| Chaney | Joseph | Non-Voting | FBI | Special Agent |
| Chari | Bharath | Advisory | Deloitte | Cyber Risk Services |
| Chrislip | Chris | Advisory | EICORP | Senior Cybersecurity Architect |
| Chu | Tony | Voting Designee, Advisory | Indiana Department of Revenue | Chief Information Security Officer |
| Clifton | Brandon | Voting Designee, Advisory | Indiana Secretary of State | Deputy Secretary and Chief of Staff |

| | | | | |
|---|---|---|---|---|
| Cloud | Matthew | Advisory | Ivy Tech Community College of Indiana-Lake County Campus | Director of Cybersecurity Grants, Asst. Prof. of Data Analytics, and Dept. Chair School of IT and Criminal Justice. |
| Cochrane | Douglas | Contributing | Integrated Public Safety Commission | Director of Network Services |
| Cook | Rhonda | Voting | Accelerate Indiana Municipalities | Deputy Director |
| Cox | Stephen | Voting | Indiana Department of Homeland Security | Executive Director |
| Creech | Bill | Contributing | Immedion | Sales Executive |
| Cudby | Joe | Advisory | MXL Consulting | Chief Executive Officer/Principal |
| Dantzler | Will | Guest | Rofori Corp | Principal Consultant |
| Davidson | John | Non-Voting | FBI | Special Agent |
| Davis | Philip | Advisory | Community Health Network | Director, IT Risk and Compliance |
| Day | David R. | Advisory | MISO Energy | Consulting Information Security Analyst |
| Dessuit | Frank | Advisory | NIPSCO | Ops Technology and Security Manager |
| Dietz | J. Eric | Contributing | Purdue University | Professor-Computer and Information Technology |
| Dignin | Kelly | Advisory | Integrated Public Safety Commission | Executive Director |
| Dimon | Philip | Contributing | Indiana Department of Revenue | Information Security Manager |
| Dingman | Stephanie | Guest | Aon Risk Services Central | Managing Director – Cyber Solutions (Cyber/E&O Broking) |
| Dittmer | Robert | Advisory | Government Performance Solutions, LLC | Senior Consultant |
| Dlug | Beth | Voting Designee, Advisory | Allen County Election Board | Elections Director |
| Donahue | Matthew | Advisory | Consultant | Consultant |
| Driskell | Debbie | Contributing | Indiana Township Association | Executive Director |
| Ehrenberg | Jim | Advisory | Indiana Office of Technology | General Counsel |
| Ehringer | David | Voting | Rolls Royce | Business Manager for IT Security |
| Ellis | Greg | Advisory | Indiana Chamber of Commerce | Vice President, Energy and Environmental Policy |
| Enriquez | Tony | Non-Voting | US Department of Homeland Security | Cybersecurity Advisor |

| | | | | |
|---|---|---|---|---|
| Ferdon | Mary | Advisory | City of Columbus | Executive Director Administration and Community Development |
| Ferrante | Anthony | Advisory | FTI Consulting | Global Head of Cybersecurity, Senior Managing Director |
| Fite | Tom | Advisory | Indiana Department of Financial Institutions | Director |
| Foltz | Jeramy | Advisory | Tech Mahindra | Developer – Team Lead |
| Foreman | Jaimie | Advisory | City of Carmel Water, INWARN | Drinking Water Regulatory Compliance Administrator |
| Frank | Michael | Advisory | Anderson University | Professor of Political Science |
| Fredland | Valita | Advisory | Community Health Network | Senior General Counsel |
| Funk | Michelle | Advisory | Indiana Utility Regulatory Commission | Senior Utility Analyst |
| Garmon | Joe | Advisory | Wabash Valley Power | Director of IT Policy and Cyber Security |
| Gasstrom | John | Advisory | Indiana Electric Cooperatives (IEC) | Chief Executive Officer |
| Giles | Clark | Advisory | City of Indianapolis | Chief Technical Officer |
| Gilroy | Rose | Advisory | Indiana National Guard | J36 Defensive Cyber Programs |
| Goldsmith | Reid | Advisory | Indianapolis International Airport | Senior Director Information Technology |
| Gonzales | Jose | Guest | La Voz | Vice President |
| Goodlink | George | Advisory | Lake City Bank | Director |
| Goodwin | Travis | Advisory | Indiana Department of Environmental Management | Senior Environmental Manager, Security in Counter Terrorism Coordinator |
| Gramling | John | Guest | Hendricks County Government Center | Application Support/Telecom Administration |
| Greene | John | Advisory | New Lisbon Telephone Company | Chief Executive Officer |
| Gregg | John | Advisory | Accelerate Indiana Municipalities | Grassroots Legislative Advocate |
| Grennes | Bob | Voting | Indiana Department of Revenue | Commissioner |
| Groves | Justin | Guest | iLab | Client Solutions |
| Grudzinski | Walter | Guest | PwC | Director and Global Head, Business Continuity and Disaster Recovery |
| Guarente | Tom | Advisory | DeepInstinct | Americas Vice President |
| Hackett | Jeffrey (Col) | Voting Designee, Advisory | Indiana National Guard | External Affairs and Alliances |

| | | | | |
|---|---|---|---|---|
| Hadley | Ryan | Voting Designee, Advisory | Indiana Utility Regulatory Commission | Executive Director of External Affairs |
| Harper | Bryan | Voting Designee, Advisory | Indiana State Police | Criminal Investigation |
| Harper | Meredith | Advisory | Eli Lilly and Company | CISO |
| Hart | Joni K. | Advisory | Broadband Innovation Group | Executive Director |
| Heir | Rajinder | Voting Designee, Advisory | Indiana Commission for Higher Education | Chief Technology Officer |
| Helton | Trenton | Guest | Indiana Dept. of Corrections (IDOC) | IT Support Director / Information Security Officer |
| Henry | Joseph | Non-Voting | US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency | Cybersecurity Coordinator |
| Herzog | Laura | Advisory | Hendricks County | Elections Supervisor |
| Hobgood | Lisa | Contributing | Deaconess Health System | Chief Information Officer |
| Hochstetler | Jay | Advisory | Qumulus Solutions | Vice President Security Services, Chief Information Security Officer |
| Holmes | Evan | Advisory | CenterPoint Energy | Manager, Control Systems Infrastructure and Security |
| Hormann | Douglas | Contributing | Raytheon | Platform Systems / Cyber Lead |
| Hosick | David | Advisory | Indiana Department of Homeland Security | Communications Director |
| Howell | Michele | Advisory | Aon Risk Services Central | Vice President, Business Development |
| Huston | Jim | Voting | Indiana Utility Regulatory Commission | Commissioner |
| Hyer | Sam | Voting | Indiana Governor's Office | Senior Operations Director |
| Ira | Adam | Advisory | Frost Brown Todd | Attorney |
| Jackson | Craig | Contributing | IU Center for Applied Cybersecurity Research | Program Director |
| Jain | Hemant | Voting Designee, Advisory | Indiana Office of Technology | Chief Information Security Officer |
| Jarnagin | Jordan | Guest | Ball State University VSTOP | Election Systems Certification Specialist |
| Jeffers | Chris | Advisory | Indiana Economic Development Corporation | PTAC Director |
| Jirik | Jiri | Contributing | Ivy Tech Community College | Assistant Professor - Evansville |
| Johns | Jason | Advisory | Sondhi Solutions | President |
| Johnson | Jason | Advisory | Parkview Health | IS Manager |

| | | | | |
|---|---|---|---|---|
| Johnston | Kathleen | Advisory | Michael I. Arnolt Center for Investigative Journalism, Indiana University | Founding Director |
| Justice | Connie (Dr.) | Advisory | IUPUI | Professor |
| Keller | John (Dr.) | Advisory | Indiana Department of Education | Chief Information Officer, IT |
| Keyler | Dawn | Advisory | Wessler Engineering, AWWA, InWARN | Project Analyst II,Wessler Engineering; Vice Chair of Indiana Section AWWA Emergency Response Committee; and Secretary for InWARN |
| Kiilu | Joshua | Guest | Indiana Department of Homeland Security | Emergency Services Program Manager |
| Kilaru | Manikantesh | Guest | Ball State University VSTOP | VSTOP/ IT Specialist |
| King | Brad | Contributing | Indiana Election Commission | Election Division Co-Director |
| Knies | John | Contributing | Lumen | Director Information Security |
| Kochevar | Matthew | Contributing | Indiana Election Division | Co-General Counsel |
| Koressel | Jake | Advisory | Indiana Department of Education | Computer Science Specialist |
| Korty | Andrew | Advisory | Indiana University | Chief Information Security Officer |
| Krebs | Victoria | Advisory | AT&T | Professional Cybersecurity |
| Krevda | Stefanie | Voting Designee, Advisory | Indiana Utility Regulatory Commission | Commissioner |
| Kroft | Kent | Contributing | Tippecanoe County | Chief Information Officer |
| LaChat | Owen | Contributing | Northwest | VP,Technology Infrastructure and Security Management |
| Lacy | Peter | Contributing | Indiana Bureau of Motor Vehicles | Commissioner |
| Langelier | Mike | Contributing | TechPoint | President |
| Langley | Bryan | Voting Designee, Advisory | Indiana Economic Development Corporation | Senior Vice President of Defense |
| Lederman | Jaci | Guest | Vincennes University | Chair<br>Information Technology Department |
| Lefever | David | Guest | Mako Group | Chief Executive Officer |
| Lewis | Landon | Voting Designee, Advisory | Pondurance | Chief Executive Officer |
| Linder | Jared | Advisory | Family and Social Services Administration | Chief Information Officer |

| | | | | |
|---|---|---|---|---|
| Lizza | Meredith | Voting Designee, Advisory | Indiana Governor's Office | Operations Director |
| Lodin | Steve | Advisory | Sallie Mae Bank | Senior Director, Cybersecurity Operations |
| Loepker | Mark | Advisory | Insure | Director |
| Lohrentz | John | Advisory | Munster Police Department | Intelligence Analyst / Digital Forensic Analyst |
| Lowden | Rob | Voting | Indiana University | Chief Information Officer |
| Lubbers | Teresa | Voting | Indiana Commission for Higher Education | Commissioner |
| Lubsen | Graig | Advisory | Indiana Office of Technology | Director of Communications |
| Lucas | John | Voting | Citizens Energy Group | Vice President, IT |
| Lyle | George | Contributing | Purdue University | Senior IT Security Risk Analyst |
| Lyles | Dale (BG) | Voting | Indiana National Guard | Adjutant General |
| Mabry | Kevin | Advisory | Sentree Systems, Corp. | Chief Executive Officer |
| Mackey | William | Advisory | Indiana State University | Instructor |
| Martz | Jeff | Advisory | Health and Hospital Corporation | Chief Information Security Officer |
| Mathis | Dan | Advisory | Indiana Office of Technology | Compliance Manger |
| Mays | Lindsey | Advisory | Indiana Secretary of State | IT Director |
| McCullough | Cliff | Advisory | Family and Social Services Administration | Chief Privacy Officer |
| McDonald | John | Guest | Clear Object | Chief Executive Officer |
| McGrath | Danielle | Voting | Indiana Energy Association | President |
| McGraw | Michael | Advisory | McGraw Consulting Group LLC | Senior Consultant |
| McGuinness | Joe | Contributing | Indiana Department of Transportation | Commissioner |
| Meadors | Joe | Advisory | Gaylor Electric Inc | Vice President of Information Services |
| Merkner | Karl | Advisory | United Federal Credit Union | Security Engineer |
| Mertens | Chris | Advisory | Hamilton County | Director of Information Technology |
| Middleton | Robert | Guest | FBI | ASAC |

| | | | | |
|---|---|---|---|---|
| Miller | Scott | Advisory | Citizens Energy Group | Manager of Security and Compliance |
| Mitchell | Kelly | Advisory | State Treasurer | Treasurer |
| Moore | Jason | Guest | Indiana Office of Technology | Senior Information Security Engineer |
| Moorhead | Philip | Contributing | Ivy Tech Community College | Adjunct Professor |
| Moran | Mary | Advisory | Indiana Department of Homeland Security | Response and Recovery Director |
| Mosley-Romero | Chetrice | Voting; IECC Director | State of Indiana | Program Director |
| Ndow | Emmanuel | Advisory | Marion General Hospital | Chief Information Officer |
| Neel | David | Contributing | CyberTek Engineering | Chief Technical Officer |
| Neely | Dewand | Advisory | Eleven Fifty Academy | Chief Operating Officer |
| Neth | Bob | Advisory | Evansville Water and Sewer Utility | Water Distribution Manager |
| Nevers | Frank | Advisory | Franciscan Alliance, Inc. | Security Program Manager |
| Newman | Anthony | Voting Designee, Advisory | Purdue University | Chief Information Security Officer |
| Nussmeyer | Angela | Contributing | Indiana Election Commission | Election Division Co-Director |
| Odum | Matt | Advisory | Briljent, LLC | President |
| O'Hara | Brian | Advisory | BTO Associates, LLC | President/CEO |
| Ortiz | Jason | Advisory | Pondurance | Senior. Product Engineer |
| Owen | Dan | Advisory | Sexton's Creek | Associate |
| Owens | Molly | Guest | Ball State University VSTOP | Project Specialist |
| Parker | Mitchell | Voting | IU Health | Executive Director, Information Systems |
| Payne | Fred | Voting | Indiana Department of Workforce Development | Commissioner |
| Pelletier | Ronald W. | Voting | Pondurance | Founding Partner |
| Phelps | Tasha | Advisory | Phelco Technologies, Inc. | President |
| Pirau | Ron | Advisory | Archdiocese of Indianapolis | Chief Information Officer |

| | | | | |
|---|---|---|---|---|
| Poliquin | Daniel | Advisory | Deloitte | Cyber Risk Services |
| Pomper | Gale | Guest | NetworkNow! | Consultant |
| Potchanant | Joe | Advisory | Indiana University - REN-ISAC | Director of Member Services and Support |
| Prostko | Robert | Advisory | Allegion, plc | Deputy General Counsel, Cybersecurity and Intellectual Property, and Chief Privacy Officer and Principal at Allegion Ventures |
| Putnam | Reid | Advisory | Gregory & Appel Insurance | Vice President, Commercial Insurance |
| Rapp | Douglas | Advisory | Cyber Leadership Alliance | President |
| Ravenna | Leon | Advisory | KAR Global | Chief Information Security Officer |
| Redman | Justin | Advisory | Citizens Energy Group | Manager Water System Control and Planning |
| Renick | Timothy | Contributing | City of Carmel | Director of Information and Communications Services |
| Reuter | Ed | Advisory | Indiana Statewide 911 Board | Executive Director |
| Reynolds | M. Brent | Advisory | Naval Surface Warfare Center (NSWC) | Chief Scientist for Cybersecurity |
| Reynolds | Stephen | Advisory | Ice Miller | Partner |
| Richhart | Robert | Voting Designee, Advisory | Hoosier Energy REC | Chief Technology Officer |
| Ritchey | Angie | Advisory | Lake City Bank | Senior Vice President, Chief Technology Officer |
| Roberts | David | Voting Designee, Advisory | Indiana Economic Development Corporation | Vice President, Chief Innovation Officer, Business Development |
| Roeder | John | Voting | Lt. Governor's Office | Director of Legislative Affairs & Parliamentarian |
| Rogers | Marcus | Advisory | Purdue Polytechnic | Professor/Executive Director Cybersecurity Programs/Chief Scientist HTCU |
| Rogers | Marc | Advisory | Purdue | Executive Director Purdue Cyber Apprenticeship Program (PCAP) |
| Rogowski | Peri | Advisory | Indiana Department of Homeland Security | State Planning Director |
| Rogowski | Peri | Contributing | Indiana Department of Homeland Security | State Planning Director |
| Rokita | Todd | Voting | Indiana Attorney General | Attorney General |

| | | | | |
|---|---|---|---|---|
| Romero | Joseph | Advisory | IU Health | Emergency Preparedness Program Manager |
| Ross | Michael | Advisory | Indiana Criminal Justice Institute | Behavioral Health Division Director |
| Rudd | Scott | Voting Designee, Advisory | Lt. Governor's Office | Director of Broadband Opportunities |
| Rupel | Johnathan (CPT) | Advisory | Raytheon | Cyber Engineer |
| Salahieh | Rami Maximus | Advisory | Ivy Tech Community College, Valparaiso, NIISSA | CSIA Program Chair, CSOC Valpo Director |
| Scarbro Kennedy | Valinda | Advisory | IBM | HBCU Strategist |
| Schmelz | Pam | Advisory | Ivy Tech Community College | Chair, School of Information Technology |
| Schmidt | Eric | Advisory | Eskenazi Health | Information Security Officer |
| Schroeder | Alyssa | Guest | Indiana Department of Homeland Security | Deputy Legislative Director, Legal Services |
| Schroers | Steven | Advisory | Winston and Strawn, LLP | Technical Support Supervisor |
| Shemroske | Ken | Advisory | University of Southern Indiana | Associate Professor of Computer Information Systems |
| Silbaugh | Chris | Advisory | Rolls Royce | Senior Security Strategy Officer |
| Skalon | Dave | Advisory | Indiana National Guard | Chief Information Officer |
| Solero | Dan | Voting | AT&T | Security Director |
| Souza | Diego | Advisory | Cummins, Inc. | Global Chief Information Security Officer |
| Souza | Tony | Advisory | Duke Energy | Director, Cybersecurity Architecture, IT/OT & TVM |
| Stahl | Tad | Advisory | IN-ISAC / Indiana Intelligence Fusion Center | Director / Deputy Director for Cyber Intelligence |
| Staton | Jim | Voting | Indiana Economic Development Corporation | Secretary of Commerce |
| Stouder | Kevin | Advisory | Indiana Department of Financial Institutions | IT Examiner, IT Program Lead |
| Sturgeon | Nick | Advisory | IU Health | Director, Information Security |
| Sullivan | Holli | Voting | Indiana Secretary of State | Secretary of State |
| Swearingen | Mark | Advisory | Hall, Render, Killian, Heath & Lyman, P.C. | Shareholder |
| Swearingen | Brad | Voting Designee, Advisory | Rolls Royce | Director of Cybersecurity, Defense Products |

| | | | | |
|---|---|---|---|---|
| Swetnam | Douglas | Voting Designee, Advisory | Indiana Office of Attorney General | Section Chief – Data Privacy and Identity Theft Unit |
| Swick | Steve | Contributing | American Electric Power (AEP)/Indiana Michigan Power (I&M) | Chief Security and Privacy Officer |
| Taylor | Curtis | Advisory | Wabash Valley Power | Executive Vice President, Technology Services |
| Taylor | Nick | Contributing | Netlogx | Chief Information Security Officer |
| Terrell | Alan | Contributing | Indiana Rural Broadband Association | President |
| Thompson | JJ | Advisory | Sophos | Senior Director Managed Threat Response |
| Tooley | Cliff (GEN) | Voting | Indiana Economic Development Corporation | Director |
| Torres | Lori | Voting Designee, Advisory | Indiana Attorney General | Chief of Staff |
| Tucker | Jeff | Voting Designee, Advisory | Indiana Department of Workforce Development | Chief Information Officer |
| Turner | Larry | Voting Designee, Advisory | Indiana State Police | Lt. Colonel, Office of the Assistant Superintendent |
| VanZee | Andrew | Advisory | Indiana Hospital Association | Vice President of Regulatory and Hospital Operations |
| Vare | Todd | Advisory | Barnes & Thornburg LLP | Partner |
| Vespa | Tony | Advisory | Vespa Group, LLC | Owner |
| Vuppalanchi | Deepika | Advisory | Syra Health | CEO |
| Wasky | Mark | Contributing | Indiana Economic Development Corporation | Vice President & Counsel, Government & Community Affairs |
| Watkins | David | Advisory | Indiana Economic Development Corporation | SBDC State Director |
| Weirick | Jon F. | Voting Designee, Advisory | City of Ft Wayne | Senior Program Manager of Automation |
| Welch | Von | Advisory | Indiana University | Associate Vice President for Information Security |
| Werner | Kyle | Voting Designee, Advisory | Crane | Strategic Director |
| Wessler | Martin | Advisory | Wessler Engineering | Chief Executive Officer |
| Whitham | Jonathan | Guest | Indiana Department of Homeland Security | General Counsel and Legislative Director |

| | | | | |
|---|---|---|---|---|
| Whitmore | Erica | Contributing | Anthem, Inc. | Senior Security Risk and Intelligence Analyst |
| Wichlinski | Robert J. | Advisory | Great Lakes Labs, LLC | Executive Vice President and General Manager |
| Winslow (BG) | Timothy | Voting Designee, Advisory | Indiana National Guard | Director of the Joint Staff |
| Wiser | Jeff | Guest | U.S. Dept. of Homeland Security, Indiana Intelligence Fusion Center (IIFC) | USDHS |
| Wright | Carolyn | Advisory | Indiana Municipal Power Agency | Vice President, Government Relations |
| Wuellner | Mark | Advisory | Indiana Bond Bank | Executive Director |
| Yager | Stephanie | Voting | Indiana Association of County Commissioners | Executive Director |