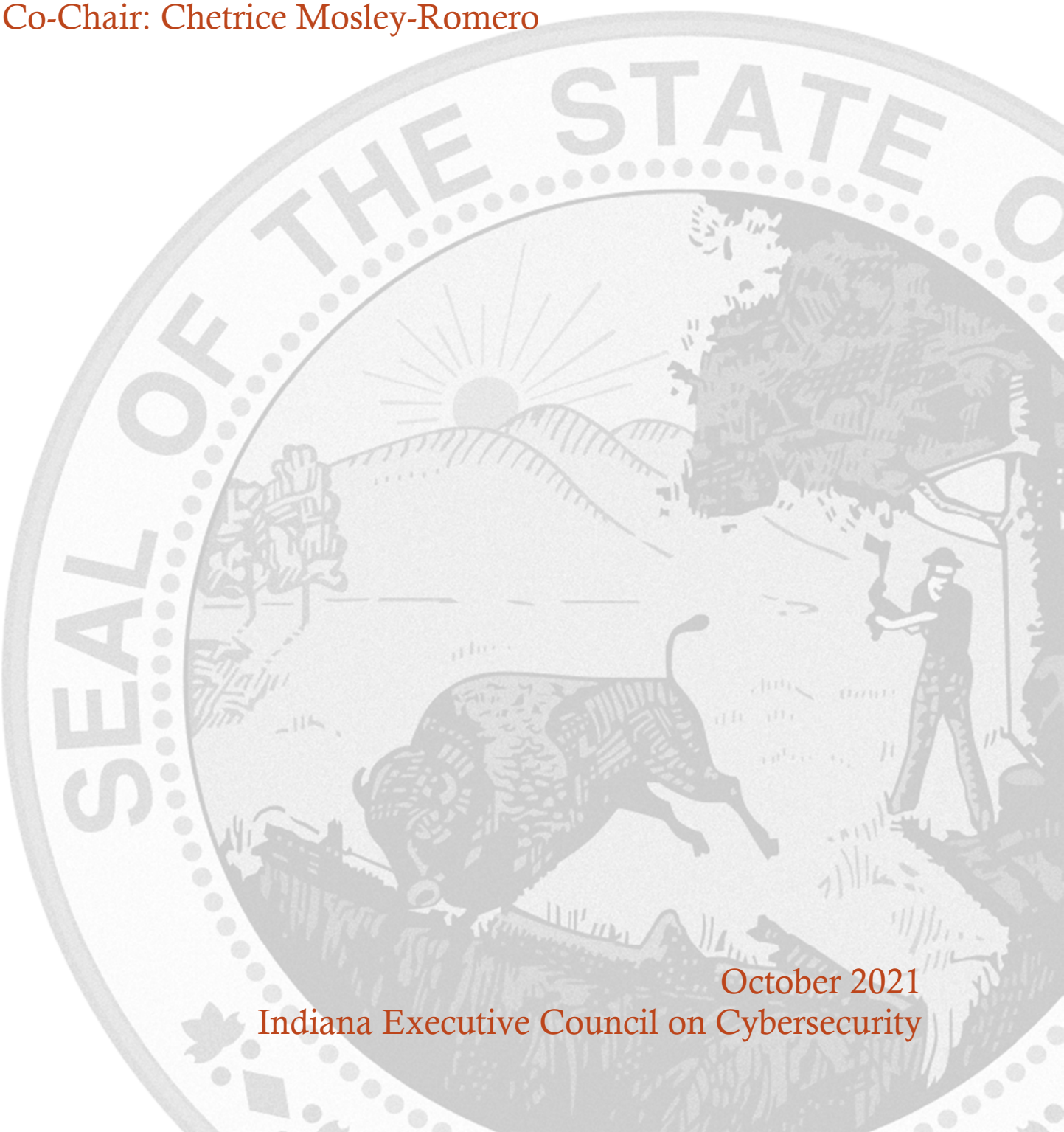
STATE AND LOCAL GOVERNMENT COMMITTEE STRATEGIC PLAN

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: a. finalize the program matrix b. define the matches of functions of local government to the source materials for the program 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: a. Pare down the functions b. Plan to give products to locals, matching functionality to level to resources c. Workshop template plan, POCs, assignments, etc. d. Communicate plan to the locals 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 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?

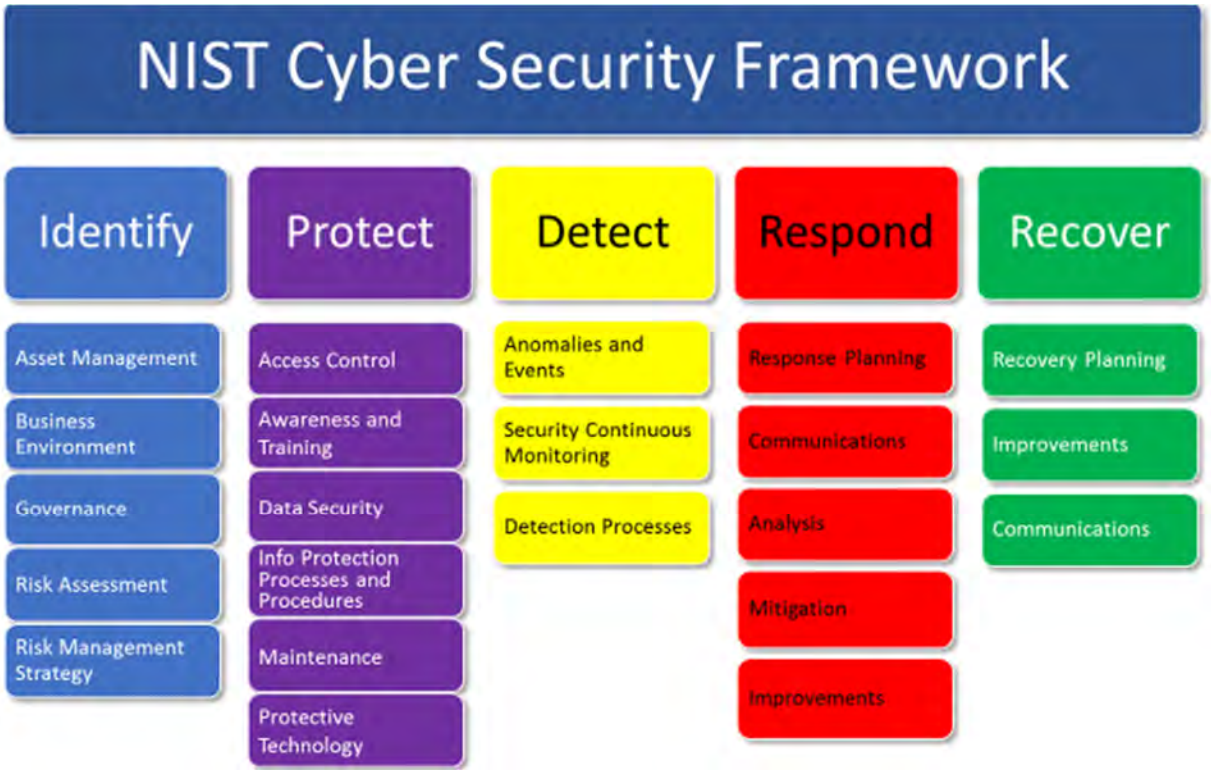
☐No ☒ Yes

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.

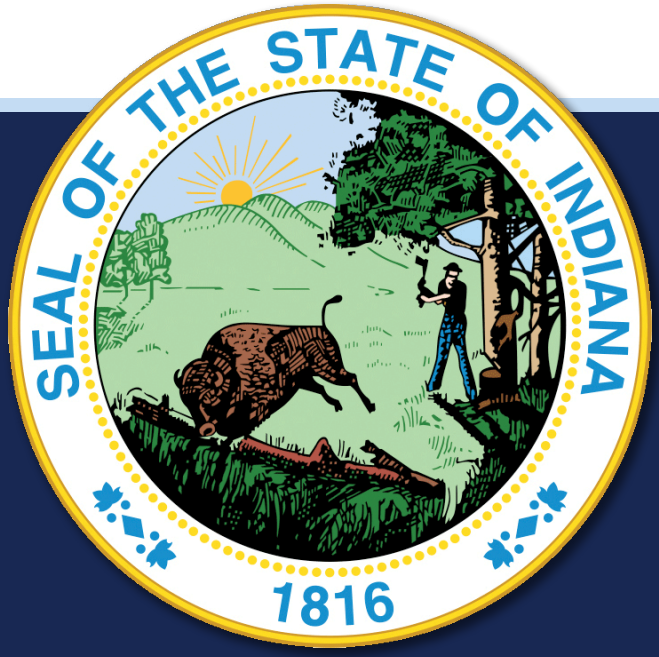
ARTICLE 6 – NON-EXCLUSION PROVISION

- 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,

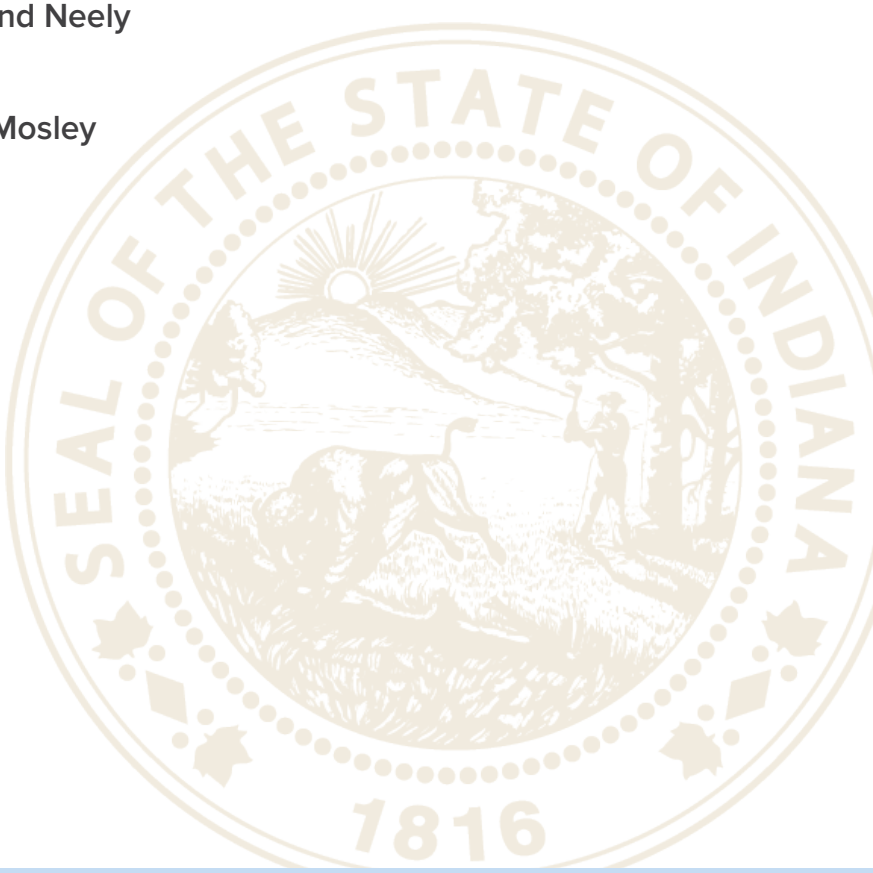
Executive Director Bryan Langley
Indiana Department of Homeland Security

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

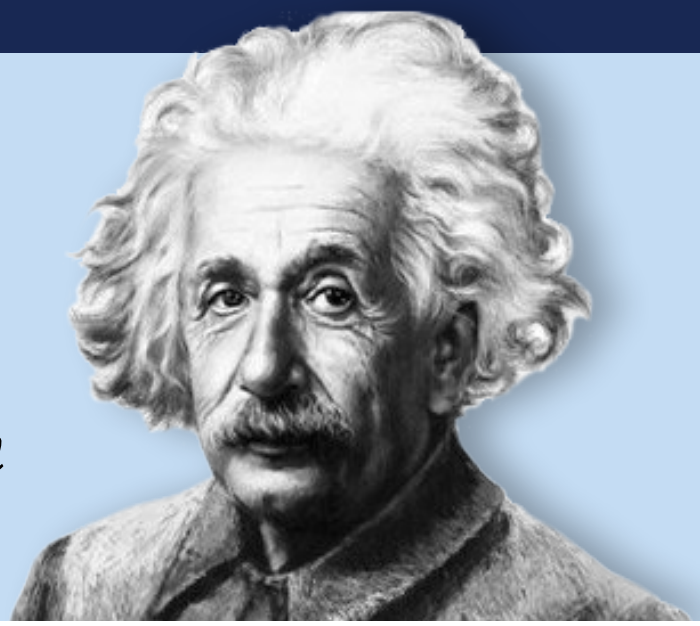
Table of Contents (continued)

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.

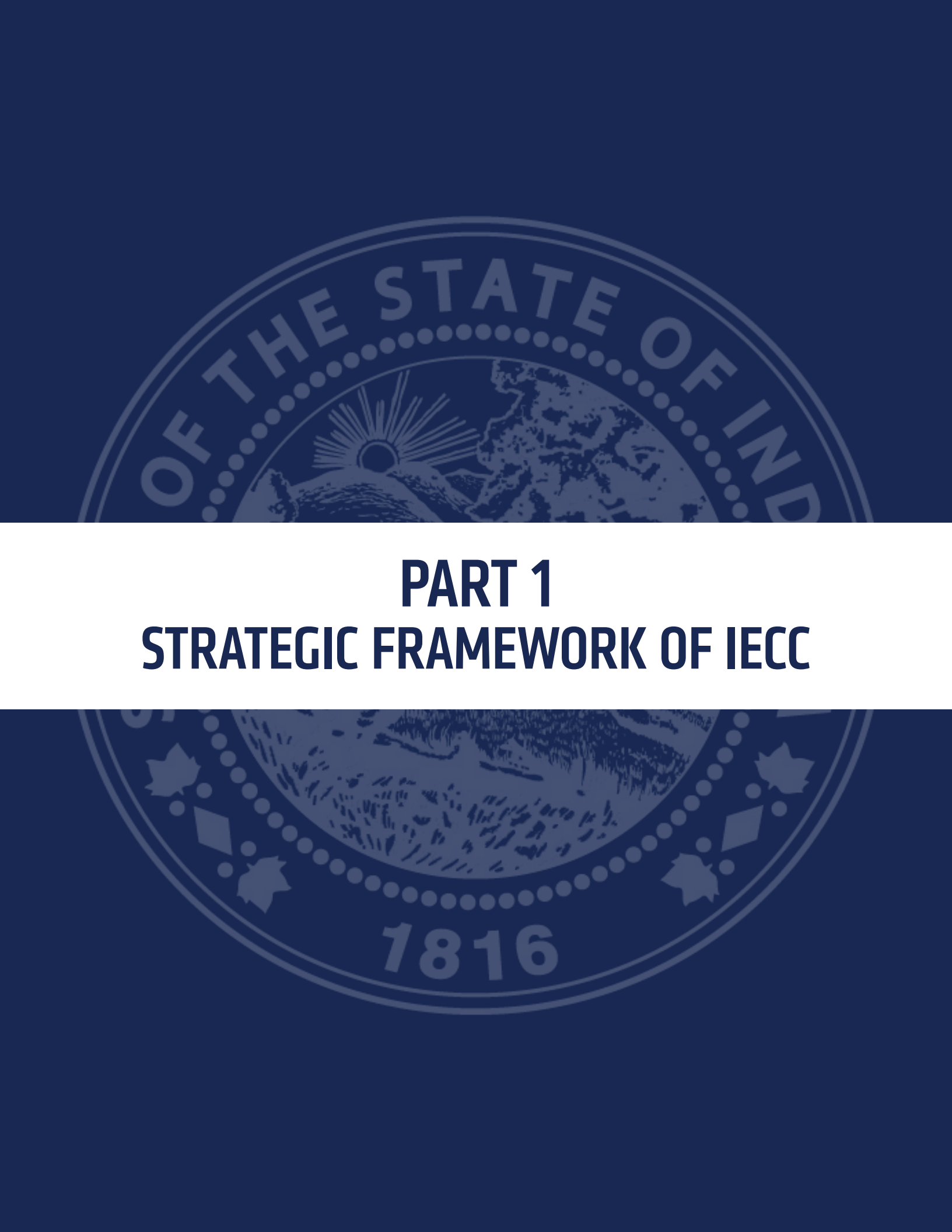
Part One is the Council's strategic framework. It provides the background of the Council, establishes high-level cybersecurity goals, presents the composition of membership, and addresses how it has met the objectives of Indiana Governor Eric J. Holcomb's Executive Order.

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.



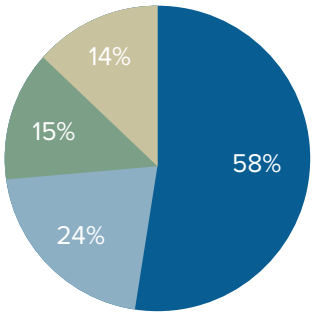
PART 1
STRATEGIC FRAMEWORK OF IECC

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.

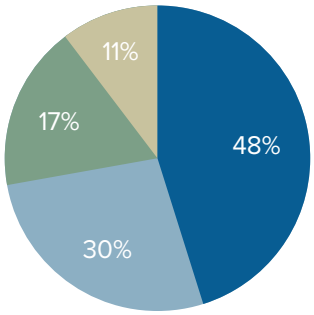
In fact, the 2018 Verizon Data Breach Investigations Report found the victims of breaches to be 58 percent small businesses, 24 percent healthcare organizations, 15 percent accommodation and food services, and 14 percent public sector entities. Of those breaches, 48 percent occurred from hacking, 30 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.

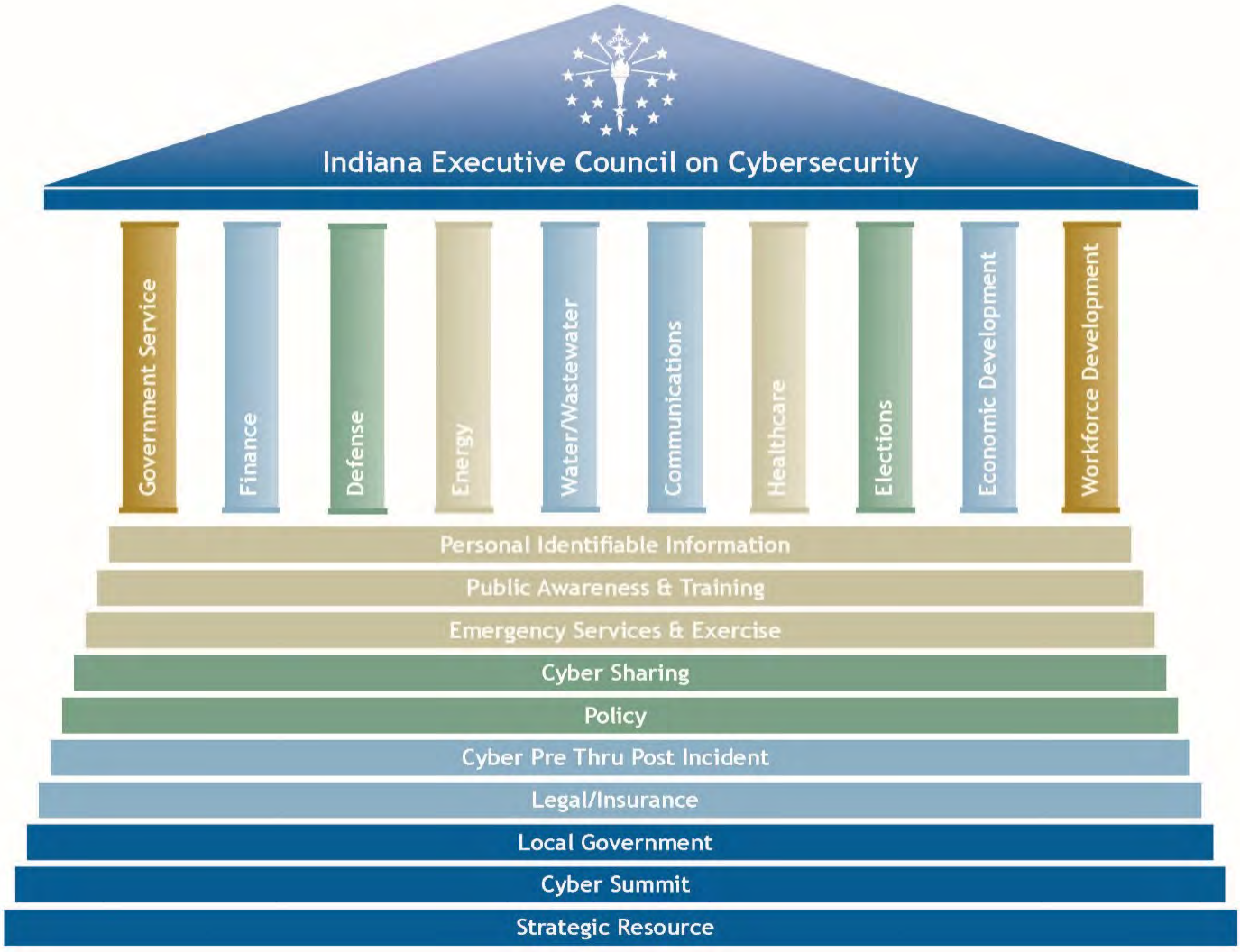


Figure 1 : IECC Strategic Breakdown

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

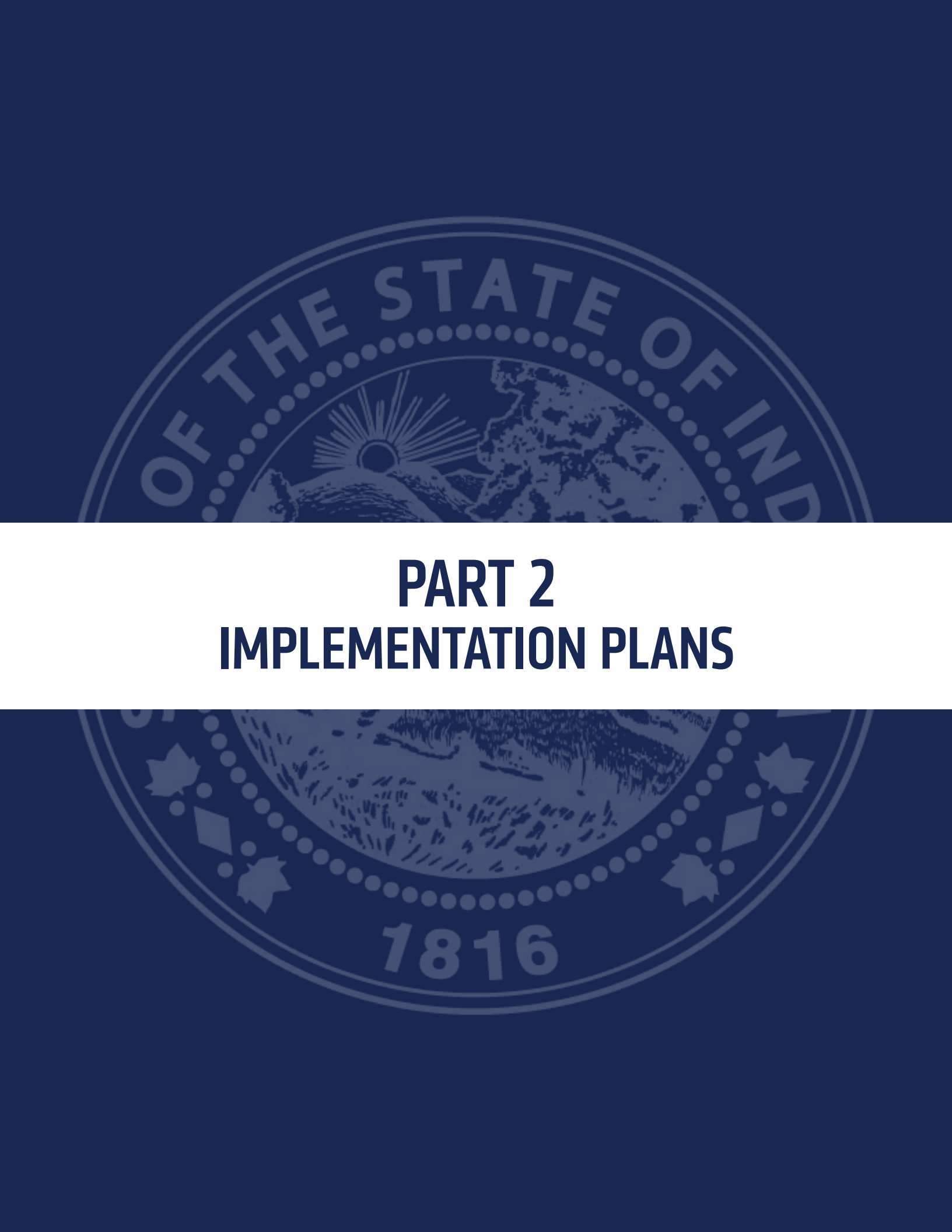
In addition, meetings, facilitated discussions, director oversight, shared online platforms, and tools, were implemented to avoid duplication of developments and deliverables, and to allow for a fully transparent process. This included a consolidated Q&A forum document that was used within and across 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 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.

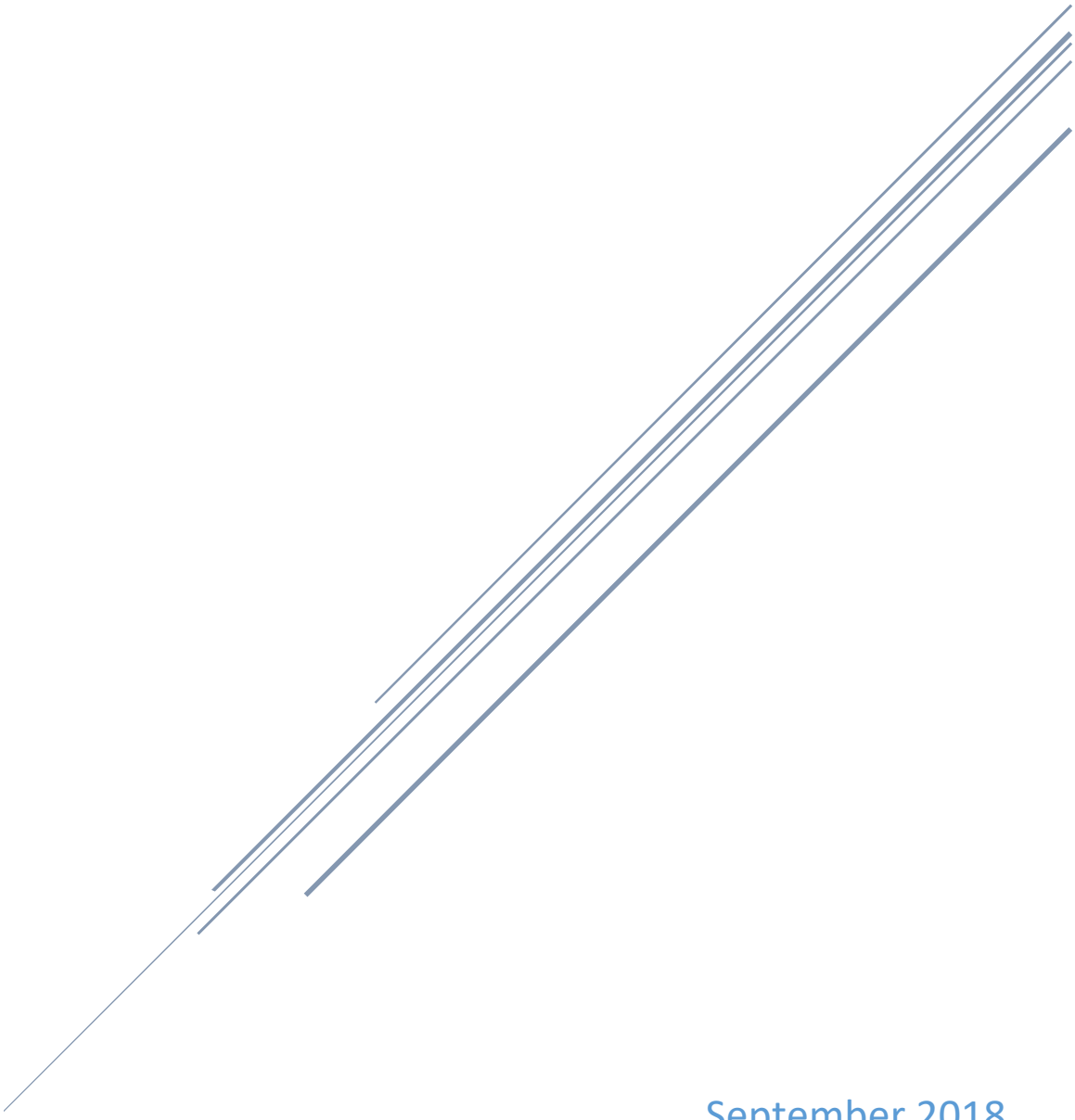
IECC MOVING FORWARD

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**	