GOVERNMENT SERVICES COMMITTEE STRATEGIC PLAN

Chair: Superintendent Doug Carter | Co-Chair: John Davidson

September 2018
Indiana Executive Council on Cybersecurity

Government Services Committee Plan

Contents

Committee Members

Committee Members

Name	**Title**	**Organization**	**Position**	**IECC Membership Type**
Doug Carter	Superintendent	Indiana State Police	CHAIR	Voting
Chuck Cohen	Captain	Indiana State Police	CHAIR – PROXY	Voting Proxy
John Davidson	Supervisory Special Agent	FBI - Indianapolis Field Office	CO-CHAIR	Non-Voting
Tad Stahl	Director / Deputy Director for Cyber Intelligence	IN-ISAC / Indiana Intelligence Fusion Center	Full Time	Advisory
Kathy Dayhoff-Dwyer	District Coordinator Liaison	Indiana Department of Homeland Security	Full Time	Advisory
Paul Dvorak	Special Agent in Charge	United States Secret Service	Full Time	Non-Voting
Doug Swetnam	Section Chief	Indiana Attorney General	Full Time	Voting Proxy
Bryan Sacks	State Chief Information Security Officer	Indiana Office of Technology	Full Time	Advisory
David Murtaugh	Executive Director	Indiana Criminal Justice Institute	Full Time	Advisory
David Tygart	J36, INNG	Indiana National Guard	Full Time	Advisory
Ted Cotterill	Chief Privacy Officer and General Counsel	Management Performance Hub	Full Time	Advisory
Ryan Myers	Sergeant	Indiana State Police	As needed	Advisory
Chris Carter	Sergeant	Indiana State Police	As needed	Advisory
Adam Krupp	Commissioner	Indiana Department of Revenue	As needed	Voting
Connie Lawson	Secretary of State	Indiana Secretary of State	As needed	Voting
Tony Enriquez	Cyber Security Advisor	USDHS	As needed	Non-Voting
Patrick McCann	Special Agent	United States Secret Service	As needed	Non-Voting

Introduction

Introduction

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

Executive Summary

Executive Summary

- **Research Conducted**
    - National Institute of Standards and Technology (NIST) Standards and Roadmap
        - https://www.nist.gov/cybersecurity-framework
    - Indiana Department of Homeland Security (IDHS) Cyber Annex
    - Indiana State Police – Indiana Intelligence Fusion Center whitepaper
    - International Association of Chiefs of Police (IACP) Cybercrime and Digital Evidence Committee
    - Association of State Criminal Investigative Agencies (ASCIA) Cybercrime Committee
    - Federal Bureau of Investigation (FBI) Cyber Division documents and resources
    - Internet Crime Complaint Center (IC3) statistical information
    - National Domestic Communications Assistance Center documents and resources
    - National White Collar Crime Center documents and resources
    - U.S. Department of Homeland Security (USDHS) Cybersecurity Guidelines and Resources
    - Presidential Executive Order on Cybersecurity
        - https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
        - https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity
    - Information Sharing and Analysis Center (ISAC) – State Comparison Research
    - Multi-State Information Sharing and Analysis Center (MS-ISAC) documents and resources
        - https://www.cisecurity.org/ms-isac/
    - U.S. Computer Emergency Readiness Team (US-CERT) documents and resources
        - https://www.us-cert.gov/
    - Collection of Indiana State Agency Cybersecurity and Identity Protection Resources (In Process)

- **Key Research Findings**
    - There is a long-standing, effective, and robust existing partnership among federal, state, and local government services in the areas of investigating and providing first response to cyber incidents and cyber emergencies in Indiana. Additionally, a plethora of established and mature government services already exist at the federal and state levels for cybersecurity. Those services are well-known among those responsible for cybersecurity both in the private and public sectors.
    - The NIST Framework for Improving Critical Infrastructure Cybersecurity ("The Framework") provides a common language for understanding, managing, and expressing cybersecurity risk, both internally and externally.
    - It is likely that state/local governmental adoption of the Framework and Roadmap will be used as a metric for determination of the availability of federal grant

    - funding in several areas. This will ensure consistency in cybersecurity among states, and between state and the federal governments.
    - The NIST Framework can be used to benchmark where a component of state/local government is at on the NIST Roadmap, both in terms of its own cybersecurity and in terms of incentivizing private business cybersecurity efforts in the state, to federal funding.

- **Committee Deliverables**
    - Indiana’s Cybersecurity Website Hub
    - Indiana Cyber Distribution/Emergency Plan

- **Additional Notes**
    - See linked sites (all retrieved on 01/02/2018)
    - The Government Services Committee members also may provide input on the Indiana Department of Homeland Security’s Cyber Annex and Indiana Office of Technology Communications Breach Protocol.

- **References**
    - See linked sites (all retrieved on 01/02/2018)

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. ISP –
        i. National leadership on cybercrime forensics
        ii. Full-time cybercrime investigators who are network intrusion and cybercrime specialists
        iii. Robust and long-standing interaction with federal law enforcement agencies in the areas of cybercrime and cybercrime forensics
        iv. National and international leadership on policy, with personnel sitting on several national and international cybercrime and digital evidence groups.
        v. Indiana Intelligence Fusion Center (IIFC) development of cybercrime intelligence component under supervision of deputy director for cyber intelligence.
    b. IDHS – Drafted cyber annex and Crit-Ex
    c. U.S. Secret Service (USSS) – Provided and continues to provide nationwide cybercrime training to law enforcement, prosecutors and judges through training and education at the National Computer Forensics Institute at Hoover, Alabama.
    d. IOT –
        i. Working to bring the State in compliance with appropriate NIST framework
        ii. Launch of Security Operations Center (SOC) and IN-ISAC
        iii. Partnership with Indiana Intelligence Fusion Center in coordination of cybercrime intelligence and IN-ISAC/SOC
        iv. Established a State-Wide Training and Awareness Program
        v. Developed and communicated an effective body of Policy and Standards based off of NIST
        vi. Established strong governance through use of processes and development of committees (Policy Management Committee; Exception Management)
        vii. Significantly expanded resource and tooling for the teams to address gaps and new threats
    e. Attorney General (AG) – Consumer protection program and Identity Theft Credit Kit
    f. Indiana Department of Revenue (IDOR): Provided annual awareness training to all employees, contractors, temps, vendors; facilitated business continuity and incident response exercises; and disseminated notifications about real-world security events, issues and best practices to the entire agency.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Year-over-year, sophistication increases in phishing attacks. There is always an opportunity to refresh training and reinforce strong security awareness.
    b. IDOR: External threats, malicious insiders, employees who fall for social engineering schemes, and sensitive data outside of the State’s protected zone.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Continued partnership among public and private sector actors responsible for cybersecurity and cyber emergency response.
    b. Coordination of messaging to private sector and local government related to available government services at the federal and state levels.
    c. Public being clearly aware of who to contact in case of a cyber emergency or incident, with the message that crime victims and those who experience potential network breaches should always contact law enforcement.
    IDOR: Funding and manpower to support security assessments and implementation of security enhancements.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Numerous federal and state laws related to responsibilities to safeguard Personal Identifying Information (PII) of third parties on networks and responsibilities to report certain crimes and events in an appropriate and timely manner.
    b. IDOR: Internal Revenue Service (IRS) publication 1075, National Institute of Standards and Technology (NIST) special publication 800-53 and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), State code, and state agency policy and standards.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Case studies include learning from other state's successes and failures in their cybersecurity efforts, including Michigan, Virginia, Maryland, and Massachusetts.
    b. Publicly available information on Madison County, Indiana malware attack.
    c. IDOR: The Information Security Research and Education (INSuRE) program researches and seeks solutions to hard security problems. INSuRE members are the US Intelligence Community, US National Laboratories, US universities and colleges such as Purdue, and State government organizations that include IOT.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. NIST Standards and Roadmap
        i. https://www.nist.gov/cybersecurity-framework
    b. IDHS Cyber Annex
    c. Indiana State Police – Indiana Intelligence Fusion Center whitepaper
    d. IACP Cybercrime and Digital Evidence Committee
    e. ASCIA Cybercrime Committee
    f. FBI Cyber Division documents and resources
    g. Internet Crime Complaint Center (IC3) statistical information
    h. National Domestic Communications Assistance Center documents and resources
    i. National White Collar Crime Center documents and resources
    j. USDHS Cybersecurity Guidelines and Resources

k. Presidential Executive Order on Cybersecurity
    i. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
    ii. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity
l. ISAC – State Comparison Research
m. MS-ISAC documents and resources
    i. https://www.cisecurity.org/ms-isac/
n. US CERT documents and resources
    i. https://www.us-cert.gov/
o. Collection of Indiana State Agency Cybersecurity and Identity Protection Resources (In Process)

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. See previous question.
    b. IDOR: The IRS requires anyone receiving Federal Tax Information (FTI) to receive security awareness training, additional security training for specific roles, and contingency and incident response training for pertinent personnel.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Develop the Indiana Cyber Emergency Plan
    b. Create a collaborative communications plan for the general public (individuals, local government, and businesses) about state and federal cybersecurity government services and resources, including centralizing information on www.in.gov/cybersecurity.
    c. Provide input to Indiana Department of Homeland Security Cyber Response Annex to the Comprehensive Emergency Management Plan.
    d. Provide input to Indiana Office of Technology Communications Breach Protocol for state agencies and recommended protocol for local government.
    e. IDOR: Year 1: Implement performance of annual security assessments and security controls for severe and significant findings. Years 3 & 5: Help vendors, partners, and tax e-filing community become compliant with DOR security; improve agency access controls, data security, and vulnerability management; and normalize annual business continuity/disaster recovery planning and testing.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. Create a collaborative communications plan for the general public (individuals, local government, and businesses) about state and federal cybersecurity government services and resources, including centralizing information on www.in.gov/cybersecurity.
    b. IDOR: The public should be apprised that DOR continuously implements tools and processes to bolster cybersecurity to protect their information, which may appear inconvenient to them. For example, we may require taxpayers logging into our applications to increase the length and complexity of their passwords.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. Many state agencies have cybersecurity-related workforce. For example, IDOR has:
        i. Total DOR Workforce as of December 2017: 751. We have 659 FTEs and 92 contractors.
        ii. Total DOR Cybersecurity Staff: 6
        iii. Total DOR Cybersecurity Staff shortfall: 0

11. **What do we need to do to attract cyber companies to Indiana?**
    a. N/A

12. **What are your communication protocols in a cyber emergency?**
    a. First call from victim or entity experiencing an emergency should be to enforcement. Enforcement will coordinate between State and federal enforcement resources. Other government services will be notified and activated ad hoc, i.e as necessary.
    b. IDOR: We communicate based on our formalized process of identifying, analyzing, responding to, and recovering from incidents to include cyber emergencies

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. NIST Framework and Roadmap
    b. IDOR: Defense in-depth: an information assurance concept in which multiple layers of security controls are placed throughout an information technology system; Initial and annual security awareness training; Phishing testing.

Deliverable: Indiana’s Cybersecurity Hub Website

Deliverable: Indiana's Cybersecurity Hub Website

General Information

1. **What is the deliverable?**
   a. Improve the Cybersecurity website (www.in.gov/cybersecurity) and make it the central hub for cybersecurity information in Indiana

2. **What is the status of this deliverable?**
   a. 100% Complete

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

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

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Revamp the Cybersecurity website for the state and incorporate the marketing of the site in the public awareness working group communications plan

6. **What metric or measurement will be used to define success?**
   a. Completion of the cybersecurity website and monitoring website traffic

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

8. **Who or what entities will benefit from the deliverable?**
    a. General public

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

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

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IOT will host the cybersecurity hub website and assist in revamping it. Other state agencies and federal agencies link to cybersecurity information.

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

13. **What are the expected challenges to completing this deliverable?**
    a. Incorporating all the resources from state and federal agencies appropriately.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Create a Project Plan with IN.Gov, IOT, and IN-ISAC to create a new website	Cybersecurity Program Director	100%	May 2018	
Develop website content	Cybersecurity Program Director and content team	100%	August 2018	
Develop website framework	IN.gov	100%	August 2018	
Test website and make edits	Cybersecurity Program Director and content team	100%	August 2018	
Develop Communications Plan	Cybersecurity Program Director	100%	September 2018	
Website launches	IN.gov	100%	September 2018	
IECC members make edits and update website	IECC	0%	January 2019 – change package #1 March 2019 and on – scheduled change packets	Ongoing effort
Implement Communications Plan	Cybersecurity Program Director	25%	September 2018 – September 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

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

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1 FTE	1 FTE	Communications /Web master	State of Indiana	N/A	
1 FTE	0	Communications and/or cybersecurity	State of Indiana	N/A	Intern to assist IOT and Cybersecurity Program Director with website development and content

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

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
IN.Gov	Services will be required to create the website in the timeframe needed	N/A	N/A	State of Indiana – Indiana Office of Technology	N/A	

Benefits and Risks

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

a. This will provide a central location for the public and a variety of stakeholders to get and receive key information surrounding cybersecurity in Indiana, including but not limited to Indiana Emergency Disruption Plan, training, toolkits, cyber events, cyber tips, self-assessments, maturity models, and federal and state resources.

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

a. This deliverable will provide the public and stakeholders a central hub for many resources that the IECC is developing that will decrease their cybersecurity risk through education, awareness, and training.

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

a. The risk of not completing this deliverable is that the many resources that the IECC is developing for the public will not be easily found. If they are not found, then stakeholders may find it more difficult to raise their cybersecurity level.

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

a. A completion of the website and meeting the milestones will be a measure of success. In addition, an increase of traffic to the website compared to the baseline of traffic to the current website will also be a measure of success.

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

a. Yes

b. **If Yes, please list states/jurisdictions**

   i. Many states do have a central hub for its cybersecurity efforts. An example is Virginia at http://cyberva.virginia.gov/ or dedicated sections of websites such as Maryland at http://doit.maryland.gov/cybersecurity/Pages/default.aspx

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. Many other states do not have a central hub for cybersecurity efforts in the state

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. Scope of project to be done by the deadline may negatively impact the deliverable.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. A state employee will need to serve as point person for all updates that will need to occur on the website.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. Indiana Office of Technology, IN.Gov web services, IN-ISAC

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. All sectors

Communications

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. General public, IECC members, state, federal, and local government, partners, legislative branch, executive branch, businesses, sectors

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

30. **What are other public relations and/or marketing considerations to be noted?**
    a. This will serve as the Central Hub for all other relative public relations and marketing on behalf of the IECC.

Evaluation Methodology

Objective 1: IECC will develop and launch a statewide cyber hub website by September 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Increase website traffic to www.in.gov/cyber by two-hundred percent by September 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Indiana Cyber Disruption / Emergency Plan

Deliverable: Indiana Cyber Disruption / Emergency Plan

General Information

1. **What is the deliverable?**
    a. Indiana Cyber Disruption/Emergency Plan

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

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Indiana Cyber Disruption/Emergency Plan created to formalize partnerships and processes to be used to communicate to stakeholders.

6. **What metric or measurement will be used to define success?**
    a. Completion of plan and communication of plan.

7. **What year will the deliverable be completed?**
    a. 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Government agencies and business stakeholders.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Emergency Services and Exercise working group, public awareness and training working group, cyber sharing working group, pre to post incident working group, and local government working group.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Law enforcement agencies (federal and state) and state agencies

12. **Who should be main lead of this deliverable?**
    a. Government Services Committee

13. **What are the expected challenges to completing this deliverable?**
    a. Getting consensus from all involved in proper notification and mass communicating it to stakeholders who would benefit from it.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Draft Plan	Tad Stahl	100%	November 2017	
Provide to Committee for review	Chuck Cohen	100%	November 2017	
Edit Plan	Cybersecurity Program Director	100%	August 2018	
Review and provide feedback on plan	Government Services Committee	75%	January 2019	
Finalize Plan	Cybersecurity Program Director	0	March 2019	
Distribute Plan	Cybersecurity Program Director	0	May 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

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

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A	N/A	State and federal agency leads	Government	N/A	Government leads will provide feedback on plan

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

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

Benefits and Risks

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

a. This plan is the external communication piece to government partners, emergency service manager, business and the general public as to who to contact during a cyber emergency and what the roles of the various stakeholders involved will be.

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

a. This deliverable will reduce the potential confusion during a cyber emergency with certain key stakeholders and the general public.

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

a. The risk of not completing this deliverable is adding to the already confused stakeholders of who to contact and when. This is especially important when there is misinformation about who to contact, when in fact law enforcement should always be the first contact made during a cyber emergency.

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

a. Completion of all milestones and a comprehensive review from key state and federal agencies is considered a success for this plan.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. Michigan has a Cyber Disruption Plan that Indiana used as a reference point in creating this plan.

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. There are other states that do not have a disruption plan. The National Governor's Association has a list.

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. Appropriate review of key state agencies in a timely manner may affect this deliverable.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

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

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

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. All sectors can use this plan as a reference point in a cyber emergency.

Communications

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. State and federal partners, local government, sector partners, associations, IECC members, emergency services partners, general public and businesses

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

   a. Yes

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

   a. None as of now.

Evaluation Methodology

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

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Supporting Documentation

Supporting Documentation

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

- Department of Revenue Government Services Research Responses

Department of Revenue

Government Services Research Responses

December 2017

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

COMMITTEE AND WORKING GROUP QUESTIONNAIRE – RESEARCH PHASE

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

Provide your questions and answers to MosleyCLM@iot.in.gov no later than ***January 2018.***

Committee/Working Group Completing Questions: Government Services Committee and Personally Identifiable Information (PII) Working Group

Person Submitting Answers: Adam Krupp, Commissioner, Indiana Department of Revenue

Email of Person Submitting: AKrupp1@dor.IN.gov

Date Submitted: December 2017

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Provided security awareness training to all FTEs, contractors, temps, and vendors at on-boarding and annually thereafter. This training apprises employees of the data they must protect, and the methods by which they must be protected.
    b. Led a Continuity of Operations plan exercise in 2014—next one projected for 2018
    c. Trained and exercised the Department of Revenue (DOR) Incident Response team and plan annually
    d. Sent periodic e-mails and published articles in agency publications apprising all DOR staff of security issues and best security practices
    e. Sent e-mails to all DOR staff apprising them of urgent real-world security issues, and how to address them (e.g., phishing messages and phone-based social engineering attacks)

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. External threats (State and non-state cyber actors, cybercriminals, cyberterrorists, etc.)
    b. Malicious insiders
    c. Employees who fall for social engineering schemes
    d. Servers containing sensitive data that reside outside of the state's protected zone (PZ)

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Funding and manpower to support security assessments and implementation of security enhancements

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Internal Revenue Service (IRS) Publication 1075
    b. National Institute of Standards and Technology (NIST) Special Publication 800-53: Using Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) for detailed security assessments
    c. Indiana Code and policies
    d. Indiana Office of Technology (IOT) policies and standards
    e. DOR policies and procedures

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. The Information Security Research and Education (INSuRE) program researches and seeks solutions to hard security problems. INSuRE members are the US Intelligence Community, US National Laboratories, US universities and colleges which include Purdue, and State government organizations including IOT.

6. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. All other state departments of revenue/taxation that receive Federal Tax Information (FTI) are required by IRS to provide:
        i. Security awareness training to all employees
        ii. Role-based training to personnel based on assigned security roles and responsibilities
        iii. Contingency training to personnel responsible for recovering backup copies of FTI
        iv. Incident response training to personnel responsible for handling and reporting security events

7. **What does success look like for your area in one year, three years, and five years?**
   a. **Year 1**
      i. Conduct security assessments
      ii. Implement security controls address severe and significant vulnerabilities and threats
   b. **Year 3**
      i. DOR, its vendors, partners, and e-filing tax community comply with DOR security requirements
      ii. Work towards the following goals
         1. All sensitive DOR servers reside in the state's PZ
         2. DOR servers reside in appropriate network segments
         3. All sensitive DOR data within the state network is encrypted at rest and in motion
         4. DOR users have least privileged access
         5. Security patching is done immediately
         6. Continuity of Operations (COOP) and Disaster Recovery (DR) plans are developed, appropriately resourced, and successfully tested
   c. **Year 5:** Achieve the following goals
      i. All sensitive DOR servers reside in the state's PZ
      ii. DOR servers reside in appropriate network segments
      iii. All sensitive DOR data within the state network is encrypted at rest and in motion
      iv. DOR users have least privileged access
      v. Security patching is done immediately
      vi. COOP and DR plans are developed, appropriately resourced, and successfully tested

8. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
   a. The public should be apprised that DOR continuously implements tools and processes to bolster cybersecurity to protect their information, which may appear inconvenient to them. For example, we may require taxpayers logging into our applications to increase the length and complexity of their passwords.

9. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
   a. Total DOR Workforce as of 17 Dec 2017: 751. 659 full-time employees (FTEs) and 92 contractors.
   b. Total DOR Cybersecurity Staff: 6
   c. Total DOR Cybersecurity Staff shortfall: 0

10. **What do we need to do to attract cyber companies to Indiana?**
    a. Unknown

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

a. DOR Employee, IOT, or anyone else identifies and reports suspicious activities to DOR Security Team

b. DOR Security Team assesses and analyzes the situation, and determines if there is an emergency

c. DOR Security Team, upon DOR Chief Information Officer (CIO) approval, takes immediate action as necessary to stop the perpetuation of damage

d. DOR Security Team develops multiple courses of action (COA) to address remaining security concerns and to recover from the event, then presents them to other members of the DOR Incident Response Team comprising DOR Chief Operating Officer, DOR Chief Information Officer, DOR Inspector General, DOR Legal Team, DOR Communications Team, and IOT Chief Information Security Officer

e. DOR Incident Response Team decides on a single course of action

f. DOR Incident Response Team briefs DOR Commissioner on the situation, actions taken, and proposed COA

g. DOR Commissioner approves COA

h. DOR Incident Response Team works with IOT to execute the approved COA

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

a. Defense in-depth: an information assurance concept in which multiple layers of security controls are placed throughout an information technology system

b. Initial and annual security awareness training

c. Phishing testing