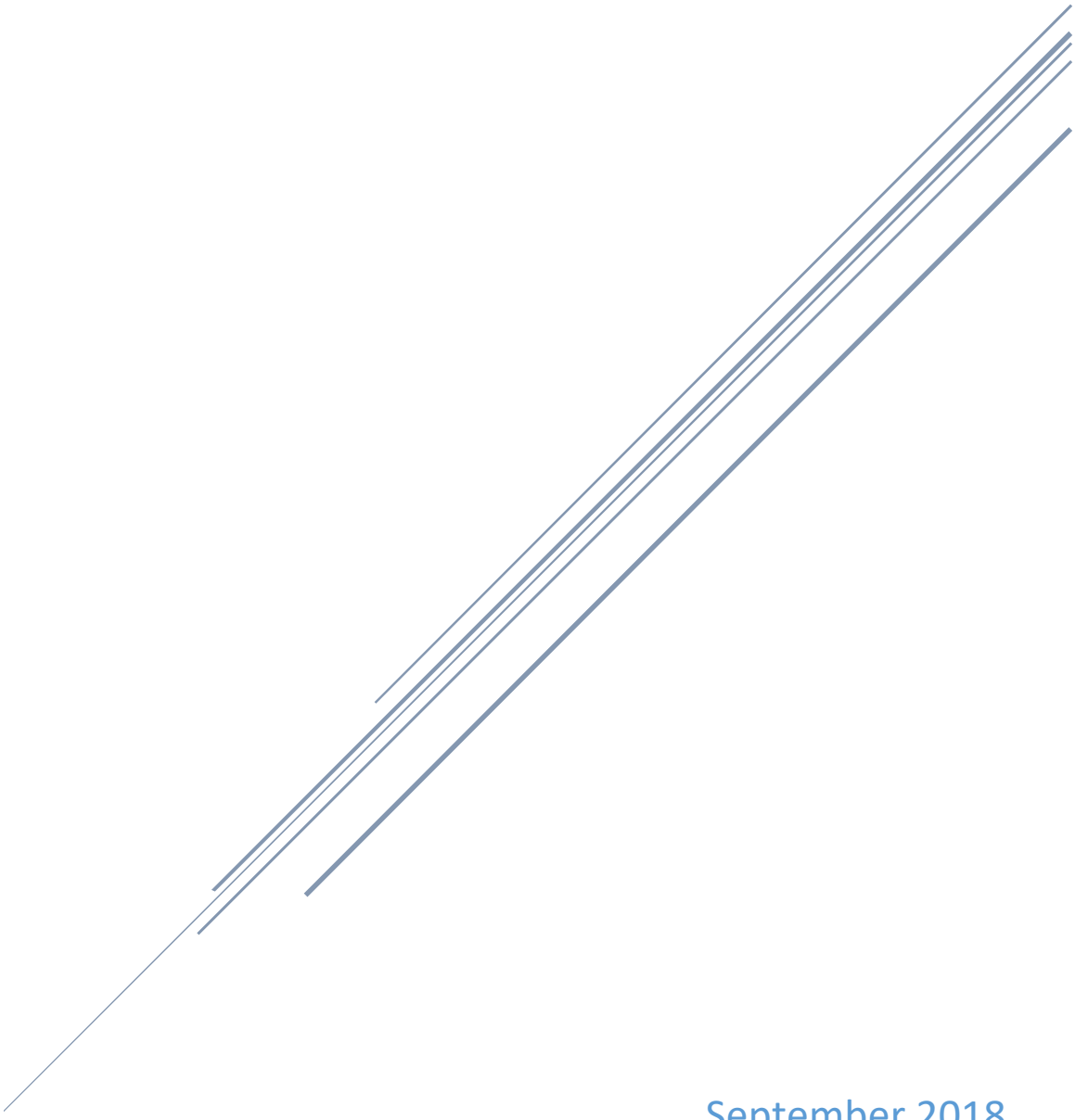
STRATEGIC RESOURCE WORKING GROUP STRATEGIC PLAN

Chair: Chetrice Mosley | Co-Chair: Scott Miller



September 2018
Indiana Executive Council on Cybersecurity

Strategic Resource Working Group Plan

Contents

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Chetrice Mosley	State of Indiana	Cybersecurity Program Director	Chair	IECC Director
Scott Miller	Citizens Energy Group	Manager of Security and Compliance	Co-Chair	Advisory
Noel Lephart	Indiana Office of Technology	Program Manager	Full Time	Advisory
Eric Dietz	Purdue	Professor, CIT	Full Time	Advisory
William Mackey	Indiana State University	Professor	Full Time	Advisory
Rich Banta	Lifeline Data Centers	Partner	Full Time	Advisory
Connie Justice	IUPUI	Professor	Full Time	Advisory
Joe Romero	IU Health	Emergency Manager	As Needed	Advisory
Brad Wheeler	Indiana University	CIO	As Needed	Advisory
Mark Bruhn	Indiana University	Associate VP of Public Safety and Institutional Assurance	Full Time	Advisory
Gerry McCartney	Purdue	CIO	As Needed	Advisory
Ron Bush	Ron Bush Consulting	Consultant	As Needed	Advisory
Ron Bushar	Mandiant	Director	As Needed	Advisory
Joe Cudby	Kinney Group	Vice President	Full Time	Advisory
Stephanie Dingman	Aon PLC	Manager	As Needed	Advisory
Matthew Donahue	LexisNexis Risk Solutions	Director	Full Time	Advisory
Michael Frank	Anderson University	N/A	As Needed	Advisory
Jose Gonzales	La Voz	Vice President	As Needed	Advisory
David Greer	Project Lead The Way, Inc.	N/A	As Needed	Advisory
Mike Langelier	Techpoint	President	As Needed	Advisory
Mark Loepker	INsURE	Director	As Needed	Advisory
John Lohrentz	Munster Police Department/NISSA	N/A	As Needed	Advisory

Thomas MacLellan	Symantec	Government Affairs	As Needed	Advisory
Dan Owen	N/A	Independent Consultant	As Needed	Advisory
Tasha Phelps	Phelco Technologies, Inc.	President	As Needed	Advisory
Chad Pittman	Purdue Research Foundation	N/A	As Needed	Advisory
Diana Williams	Project Brilliant	Director	Full Time	Advisory

Introduction

Introduction

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

Executive Summary

Executive Summary

- **Research Conducted**
  - National Governors Association (NGA)
  - National Association of State Chief Information Officers (NASCIO)
  - Purdue Homeland Security Project
  - State-to-State Comparison Research
  - Cybersecurity Prediction Reports
  - Fusions Centers
  - Information Sharing and Analysis Centers (ISAC)
  - Indiana Department of Homeland Security (IDHS)/U.S. Department of Homeland Security (USDHS)
  - Policy
  - Conferences
  - Webinars
  - Best Practices/Examples of other Councils and Boards
  - Feedback from Council members before the hiring of the Cybersecurity Program Director

- **Research Findings**
  - It was imperative to understand all aspects of the cyber ecosystem within state government. This included understanding:
    - Fusions Centers
      - https://www.dhs.gov/annual-fusion-center-assessment-and-gap-mitigation-activities
      - http://www.govtech.com/em/safety/National-Fusion-Center-Model-Is-Emerging.html
      - https://nfcausa.org/
      - https://www.dhs.gov/national-network-fusion-centers-fact-sheet
      - https://nfcausa.org/html/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers.pdf
    - Information Sharing
      - National Strategy for Information Sharing: https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/1763-2012-national-strategy-for-information-sharing-and-safeguarding-nsiss
      - ISAC state to state comparison primary research
      - See Research Executive summary for Cyber Sharing Working Group
    - National Guard – See Pre thru Post Incident Working Group Executive Summary
    - IDHS – See Emergency Services and Exercise Executive Summary
    - Federal Partnerships

- **Working Group Deliverables**
  - IECC Framework Documentation
  - IECC Scorecard

- IECC Sustainability Recommendation

- **Additional Notes**
  - **State and Other Example Websites**
    - Cyber Virginia
    - Michigan Cyber Initiative
    - Missouri Office of Cybersecurity
    - Pennsylvania
    - Washington Cybersecurity Program
    - Wisconsin Cybersecurity
    - Multistate Information Sharing and Analysis Center (MS-ISAC)

- **References**
  - Article: Presidential Cybersecurity E.O. - http://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-trump-executive-order-on-cybersecurity-just-an-opening-act.html
  - NGA Meet the Threat - https://www.nga.org/cms/meet-the-threat
  - National Association of State Chief Information Officers (NASCIO) - https://www.nascio.org/
  - PPD 41 – U.S. Cyber Incident Coordination: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
  - U.S. Computer Emergency Readiness Team (US-CERT): https://www.us-cert.gov/
  - Report: State of the States on Cybersecurity (Pell Center)
  - Memo on State Cybersecurity Governance Bodies
  - Memo on State Cybersecurity Response Plans
  - Michigan Cyber Disruption Response Plan
  - NIST Computer Security Incident Handling Guide
  - NASCIO Cyber Disruption Response Planning Guide
  - Building a Cybersecurity Workforce Pipeline

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. Crit-Ex 2016
    b. Established Governor Council on Cybersecurity – March 2016
    c. Continued Governor Council on Cybersecurity – January 2017

2. **What (or who) are the most significant cyber vulnerabilities in your area**?
    a. Critical infrastructure, businesses, and individuals

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. A comprehensive, collaborative strategic state-wide cybersecurity approach that will address:
        - Establish an effective governing structure and strategic direction;
        - Formalize strategic cybersecurity partnerships across the public and private sectors.
        - Strengthen best practices to protect information technology infrastructure;
        - Build and maintain robust statewide cyber incident response capabilities;
        - Establish processes, technology, and facilities to improve cybersecurity statewide;
        - Leverage business and economic opportunities related to information, critical infrastructure, and network security; and
        - Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Regulations vary by industry and sector.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Other State Models such as:
        - Cyber Virginia
        - Michigan Cyber Initiative
        - Missouri Office of Cybersecurity
        - Pennsylvania
        - Washington Cybersecurity Program
        - Wisconsin Cybersecurity
        - Multistate Information Sharing and Analysis Center (MS-ISAC)

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. National Governors Association
    b. National Association of State Chief Information Officers (NASCIO)
    c. Purdue Homeland Security Project – in progress
    d. State-to-State Comparison Research – ongoing

e. Cybersecurity Prediction Reports
f. Fusions Centers
g. Information Sharing and Analysis Centers (ISACs)
h. Indiana Department of Homeland Security/United States Department of Homeland Security (IDHS/USDHS)
i. Policy
j. Conferences
k. Webinars
l. Best Practices/Examples of other Councils and Boards
m. Feedback from Council members prior to the hiring of the Cybersecurity Program Director

7. What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?
   a. See question 5 and 6.

8. What does success look like for your area in one year, three years, and five years?
   a. Developing a sustainability model with appropriate resources that will continue to implement and demonstrate measurable improvement in the state's cybersecurity posture will be vital to the Council's continued success. The model will ensure that the Council continues to develop, maintain, and execute the implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which will be completed within an established timeframe over the next one, three, and five years.

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?
   a. An overall communication plan to increase cybersecurity awareness, programs, training, and education is needed.

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

11. What do we need to do to attract cyber companies to Indiana?
   a. The State's emphasis on the importance of cybersecurity will attract companies to Indiana.

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

13. What best practices should be used across the sectors in Indiana? Please collect and document.
   a. See sector specific questionnaire.

Deliverable: IECC Program Documentation

Deliverable: IECC Program Documentation

General information

1. **What is the deliverable?**
    a. IECC Program Documentation

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

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Documentation of the creation, implementation, and evaluation of the IECC, including the project plan, framework, governance, tools used, and lessons learned.

6. **What metric or measurement will be used to define success?**
    a. Completion and inclusion of the IECC Program Documentation in the final plan

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

8. **Who or what entities will benefit from the deliverable?**
    a. IECC, Governor's office, federal and state partners

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

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All, as needed

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None

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

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

Implementation Plan

---

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Determine what the Framework Document will contain	Program Director, Program Manager	100%	February 2018	
Develop draft Table of Contents	Program Manager	100%	February 2018	
Review draft TOC	Program Director, Program Manager	100%	February 2018	
Develop list of subtopics	Program Director, Program Manager	100%	March – April 2018	
Begin documenting topics and subtopics	Program Manager	100%	March 2018	
Determine document design	Program Director, Program Manager	100%	May-July 2018	
Complete Draft	Program Manager	100%	July 2018	
Final Draft approval	Program Director	100%	July 2018	
Strategic Resource WG approval process	Program Manager	100%	August 2018	
Complete documentation and Final Review	Program Director	100%	August 2018	
Integrate document into final report	Program Director, Program Manager	100%	September 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

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

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

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

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

Benefits and Risks

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

a. Providing supporting documentation of how the Council was planned, established, and governed. Sharing a repeatable framework for other organizations and states to leverage.

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

a. This framework documentation provides support for the Council's work, and will help support the organization of future Council efforts.

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

a. The organization and processes used with the Council will be lost and the future movement of the IECC support organization will have less direction and strategy. Knowledge sharing with other states and agencies will not occur.

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

a. Completion of the documentation July 2018 and Strategic Resource Working Group approval. The final Governor's proposal in late September 2018.

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

a. No
b. **If Yes, please list states/jurisdictions**
    i. N/A

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

a. No
b. **If Yes, please list states/jurisdictions**
    i. N/A. Because there are no other states doing work like the IECC.

Other Implementation Factors

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

a. Resource constraints, competing priorities, and a short timeframe.

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

a. No

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

a. N/A

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

a. Cybersecurity Program Director

27. Can this deliverable be used by other sectors?

a. No
b. **If Yes, please list sectors**
    i. It can be used by other states

Communications

---

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

a. IECC

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

a. Yes; it will be the Part 1 of the final cybersecurity strategic plan provided to the Governor September 2018

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

a. Further detailed information can be shared with internal management and those who request it, such as the National Governors Association (NGA), and other states.

Evaluation Methodology

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

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Deliverable: IECC Scorecard

Deliverable: IECC Scorecard

General information

1. **What is the deliverable?**
    a. IECC Scorecard

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

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The goal of the scorecard is two-fold. It will provide a baseline as well as a measurement of the effectiveness of the IECC deliverables as well as a more detailed cybersecurity self-assessment.

6. **What metric or measurement will be used to define success?**
    a. A sentinel sampling of all sectors completing the scorecard and self-assessment.

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

8. **Who or what entities will benefit from the deliverable?**
    a. Small and medium sector companies and local government.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Federal and private assessments.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All, as needed.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IECC partners with Purdue University

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

13. **What are the expected challenges to completing this deliverable?**
    a. Scope and participation of the scorecard.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Find an IECC partner to assist with developing the scorecard	Cybersecurity Program Director	100%	November 2017	Chose Purdue University
Conduct research of scorecards and assessments	Cybersecurity Program Director and Purdue	100%	January – April 2018	
Draft scorecard	Purdue	100%	March/April 2018	
Review Scorecard	Strategic Resources Working Group	100%	April 2018	
Review Scorecard	IECC	100%	April 2018	
Develop implementation plan	Cybersecurity Program Director and Ivy Tech Resource	100%	May 2018	
Identify sentinel pilot group	All critical infrastructure chairs as well as local government, business, and education sectors	100%	May-June 2018	
Pilot Group complete scorecard	Pilot Group	100%	June - September 2018	
Take survey on product	Cybersecurity Program Director and Purdue	0	October 2018	
Develop implementation plan for mass public	Cybersecurity Program Director and Ivy Tech Resource	0	December 2018	
Pilot Group retake scorecard	Pilot Group	0	March 2019	
Execute implementation plan for mass public	Cybersecurity Program Director	0	2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

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

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1 FTE	N/A	Cybersecurity and business	State of Indiana	IECC Partner	

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

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

Benefits and Risks

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

a. Measurement of the success of IECC efforts and deliverables and more importantly provide the public a tool (specifically small/medium size businesses and local governments) to start to identify their current cybersecurity posture. Additionally, after making improvements, this gives immediate feedback as to whether the improvement was made.

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

a. This scorecard is meant to assess current-state and address the problem areas most appropriate to the organization surveyed. By doing this at a business level and in a way that can be provided to executive leadership of a company, the scorecard could assist in prioritizing and providing a form of measurement to reducing cybersecurity risk or impact.

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

a. The state and the IECC will not have a mechanism of measuring progress of Indiana's cybersecurity posture.

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

a. Completion of the scorecard is an output success. Having 90 percent of all sentinel sample complete the scorecard.

21. **Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?**
    a. No

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. More than 30 states have a cyber council but have not provided a user-friendly scorecard that can be used by the organization, as well as a measurement for the effectiveness of the tools created by the Council.

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. Short time frame and engaging each sector.

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

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

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. It was presented to the full Council in April 2018 for input and discussion.

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

Communications

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. IECC, Government, businesses, associations, sector partners

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

30. **What are other public relations and/or marketing considerations to be noted?**
    a. No other like this.

Evaluation Methodology

Objective 1: IECC, along with Purdue University, will develop Indiana's first Cybersecurity Scorecard by May 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Objective 2: IECC, along with Purdue University, will launch Indiana's Cybersecurity Scorecard Pilot Program with 90 percent of selected organizations by September 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Objective 3: IECC, along with Purdue University, will develop a final report of Indiana's Cybersecurity Scorecard Pilot Program by May 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Deliverable: IECC Sustainability Recommendation

Deliverable: IECC Sustainability Recommendation

General information

1. **What is the deliverable?**
    a. IECC Sustainably Recommendation

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

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The IECC Sustainability Recommendation will help inform the Governor of the next steps with the IECC.

6. **What metric or measurement will be used to define success?**
    a. Adoption of the recommendation by the Governor, his office, and Council partners.

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

8. **Who or what entities will benefit from the deliverable?**
    a. Governor and IECC

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

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All, as needed

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

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

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

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Research other state approaches	Cybersecurity Program Director and IECC fellow	100%	August 2018	
Draft section to final report	Cybersecurity Program Director and IECC fellow	100%	July 2018	
Review	IECC Core Leadership	100%	September 2018	
Submit with final plan as a memo	Cybersecurity Program Director and IECC	100%	September 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No
b. **If Yes, please complete the following**

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

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

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

Benefits and Risks

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

a. Positioning the IECC for its continued success in implementing the overall statewide strategy for cybersecurity.

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

a. A sustainability plan will help the State of Indiana and partners to most efficiently continue to provide businesses and governments tools to continue lowering their cybersecurity risks.

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

a. Efforts of the IECC may slow down or become abandoned.

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

a. Completion of recommendation that provides a comprehensive review of what others have done and a variety of courses of actions Indiana can take.

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

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. There are many models to evaluate over the next several months to consider and explain in the report.

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

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. This will be determined in the research, but more than likely.

Other Implementation Factors

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

a. Resource constraints and short timeframe.

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

a. No

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

a. N/A

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

a. None

27. Can this deliverable be used by other sectors?

a. No

Communications

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

a. IECC, Governor's Office, general public

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

a. Yes

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

a. A public relations plan will be implemented highlighting the efforts of the IECC and report, which include the sustainability courses of actions.

Evaluation Methodology

Objective 1: IECC will develop a sustainability recommendation for the Council by September 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Supporting Documentation

Supporting Documentation

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

- IECC Cybersecurity Scorecard

Indiana Executive Council on Cybersecurity (IECC)

Cybersecurity Scorecard

April 2018

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

Welcome to the State of Indiana's Cybersecurity Scorecard in partnership with Purdue University!

This Scorecard should take you approximately 10-15 minutes to complete.

For your convenience, this Scorecard is a fillable PDF, can be saved with your answers, and will automatically calculate your score.

For your reference there is a Glossary of Terms on the last page with definitions for technical terms highlighted in blue lettering.

If you have any questions on this Scorecard, please email the Cybersecurity Program Director Chetrice Mosley at mosleyclm@iot.in.gov.

Name of Organization

_____

Your E-mail Address

_____

How many employees are there in your organization (full and part time)?

_____

How many employees have information technology related duties?

_____

How many employees have cybersecurity related duties?

_____

Does your organization outsource your information technology needs?

- ◯ Yes
- ◯ No

Does your organization outsource your cybersecurity needs?

- ◯ Yes
- ◯ No

Question 1

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our organization values cybersecurity.	○	○	○	○	○	○

Question 2

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.)	○	○	○	○	○	○

Question 3

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)	○	○	○	○	○	○

Question 4

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our business/organization model influences the way we approach cybersecurity.	○	○	○	○	○	○

Question 5

	I Don’t Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.	○	○	○	○	○	○

Question 6

	I Don’t Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We are familiar with the cybersecurity threats or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees.	○	○	○	○	○	○

Question 7

	I Don’t Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls.	○	○	○	○	○	○

Question 8

	I Don’t Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have **system checks** in place to make sure that our data is not compromised or changed.	○	○	○	○	○	○

Question 9

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our data is available to employees or clients when needed. (If our government or commerce site was unavailable to customers or employees, we would know what to do).	○	○	○	○	○	○

Question 10

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.	○	○	○	○	○	○

Question 11

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our cybersecurity technology (such as **antivirus**, wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data.	○	○	○	○	○	○

Question 12

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have a process in place to address a **cyberthreat**.	○	○	○	○	○	○

Question 13

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have a cyber emergency response plan in place to address a **cyberattack** on our organization.	○	○	○	○	○	○

Question 14

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
If we were impacted by a cyber emergency (e.g. **ransomware**), we know how our organization would recover our data and/or operational systems.	○	○	○	○	○	○

Question 15

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
After a **cyberthreat** or emergency, our organization will make changes to people, process, technology, etc. to improve our security.	○	○	○	○	○	○

Question 16

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our executive leadership receives periodic status, physical, and cybersecurity updates.	○	○	○	○	○	○

Question 17

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.	○	○	○	○	○	○

Question 18

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We provide our employees cybersecurity awareness and/or training.	○	○	○	○	○	○

Question 19

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We protect our business and customer information so that only the employees that need to see it, can.	○	○	○	○	○	○

Question 20

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We would know if our cybersecurity technology detected a **cyberthreat**.	○	○	○	○	○	○

Question 21

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	○	○	○	○	○	○

Question 22

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software	○	○	○	○	○	○

To find your score, please add the numbers associated with the responses for questions 1 through 22. For example, selecting "Almost Every Time (4)" has a numberical value of 4.

Your score is 0_____

Refer to the chart below to determine where you fall on the scale.

Grade	Exemplary	Accomplished	Developing	Beginning	Undeveloped
Minimum with color code	88	66	44	22	0
Range	110-88	87-66	65-44	43-22	21-0
Spread	22	21	21	21	21

Glossary of Terms

System checks- procedures, equipment, and/or periodic inspection to maintain security
Antivirus- i.e. McAfee, Norton, or Windows Defender
Cyberthreat- the possibility of a malicious attempt to damage or disrupt a computer network or system. For example, social engineered trojans, unpatched software (such as Java, Adobe Reader, Flash), and/or phishing
Cyberattack- an attack initiated from one or more computers against a website, computer system or a networked enterprise of several computers that compromises the confidentiality, integrity or availability of any computer(s) or stored information
Ransomware- a type of malware that prevents users from using their computer and displays messages requiring users to pay a ransom usually through an online payment in order to regain access to his/her computer, information, and/or system.