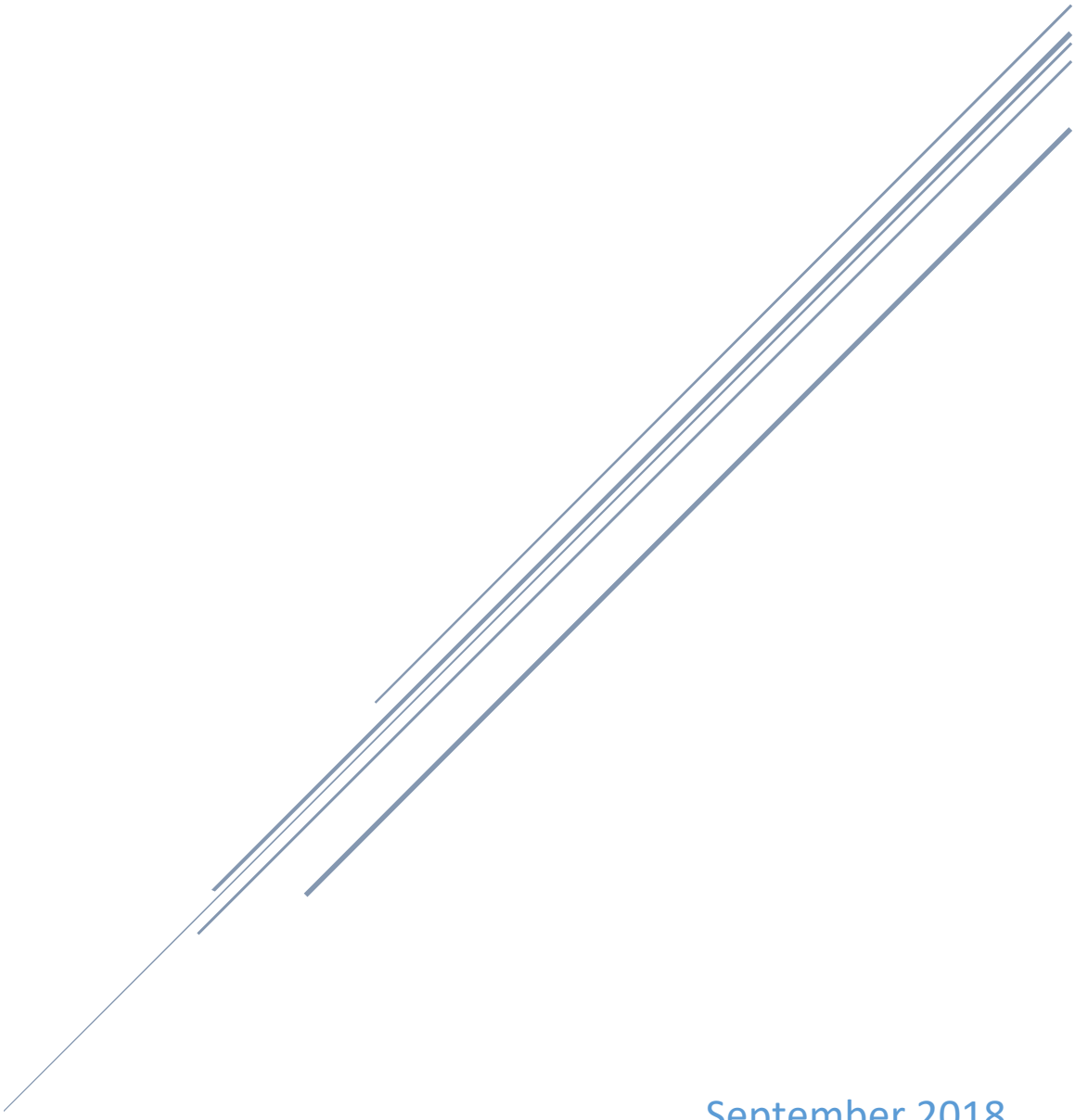
LOCAL GOVERNMENT WORKING GROUP STRATEGIC PLAN

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