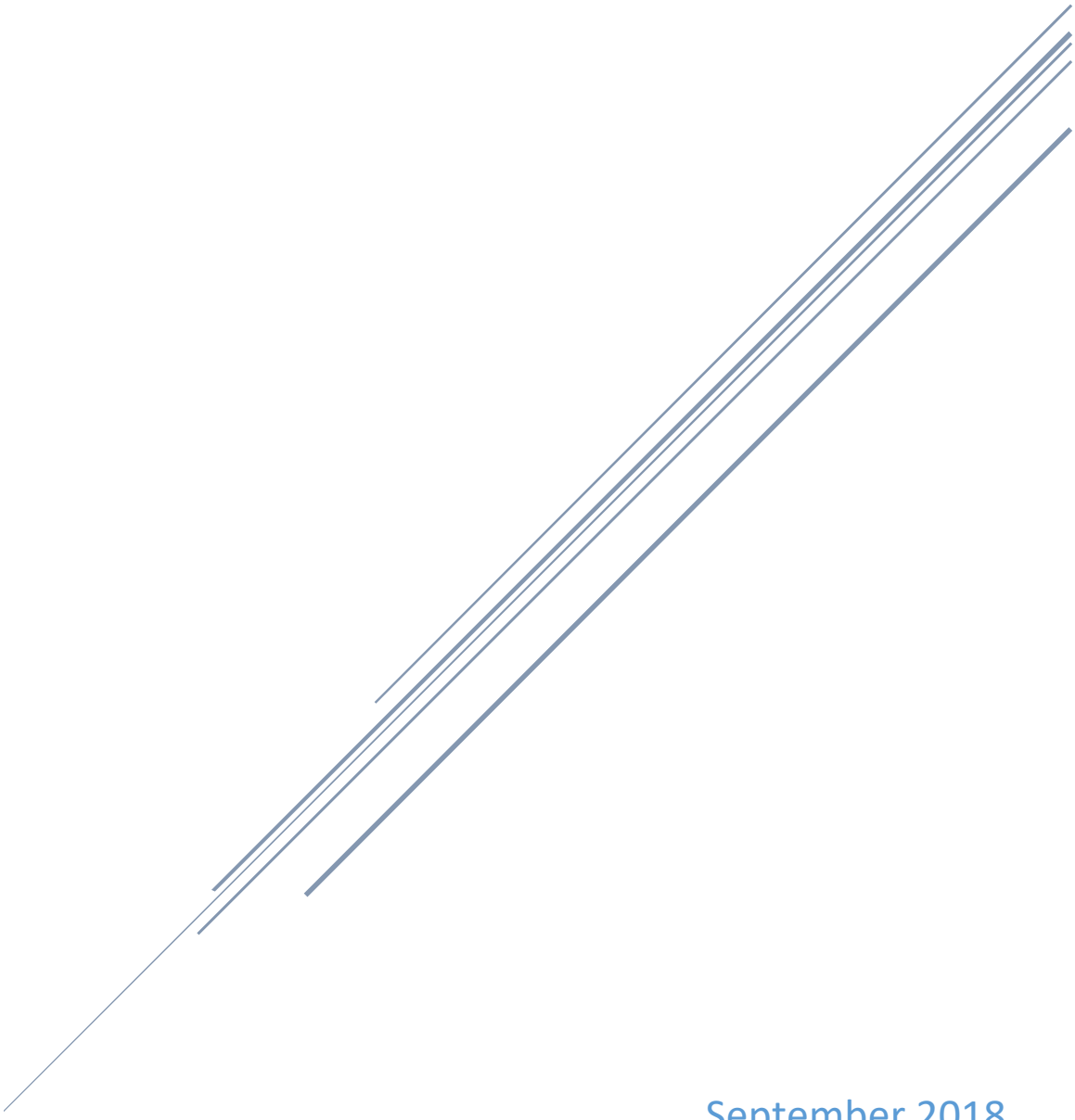
WATER & WASTEWATER COMMITTEE STRATEGIC PLAN

Chair: John Lucas | Co-Chair: Jon Weirick



September 2018

Indiana Executive Council on Cybersecurity

Water & Wastewater Committee Plan

Contents

Committee Members **4**
Introduction **6**
Executive Summary **8**
Research **10**
Deliverable: Cyber Contact **13**
General Information 13
Implementation Plan 15
Evaluation Methodology 19
Deliverable: Cyber Risk Model (Plan) **21**
General Information 21
Implementation Plan 23
Evaluation Methodology 27
Deliverable: Risk Tool **29**
General Information 29
Implementation Plan 31
Evaluation Methodology 34
Deliverable: Training Plan **36**
General Information 36
Implementation Plan 38
Evaluation Methodology 42
Deliverable: Cyber Plan Template **44**
General Information 44
Implementation Plan 45
Evaluation Methodology 49
Supporting Documentation **51**
IECC Water and Wastewater Committee Cybersecurity Plan Template 52

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
John Lucas	Citizens Energy Group	Vice President, IT, Officer	Chair	Voting
Jon Weirick	City Utilities Engineering, Fort Wayne, IN	Senior Program Manager	Co-Chair	Advisory
Steve Berube	Citizens Energy Group	Manager, Water System Control and Planning	Full Time	Voting
Cliff Campbell	Campbell Consulting, LLC	President	Full Time	Voting
Duane Gilles	Evansville Water and Sewer Utility	Water Distribution Manager	Full Time	Voting
Martin Wessler	Wessler Engineering	Chairman & CEO	Full Time	Voting
Jaimie Foreman	City of Carmel	Drinking Water Regulatory Compliance Administrator	Full Time	Voting
Connie Justice	IUPUI	Director of Cybersecurity Education and Experiential Learning	Full Time	Voting
Douglas Brock	Indiana American Water	Vice President of Operations	As Needed	Non-voting
Brian Rockensuess	Indiana Department of Environmental Management	Chief of Staff	As Needed	Non-voting
Travis Goodwin	Indiana Department of Environmental Management	Security and Counter Terrorism Coordinator	As Needed	Non-voting
Sarah Freeman	IN Utility Regulatory Commission	Commissioner	As Needed	Non-voting
Michelle Funk	IURC	Sr. Utility Analyst	As Needed	Non-voting
Jim Huston	IURC	Commissioner	As Needed	Non-voting
James Haley	City of Fort Wayne	CIO, City of Fort Wayne	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**
  - The Water/Wastewater committee conducted research in the following area:
    - Water companies / cybersecurity contact
    - Training for water companies on cybersecurity
    - Funding / legislative options for cybersecurity for water/wastewater companies

- **Research Findings**
  - Lack of contact information on cyber contacts at water companies within Indiana.
  - No risk assessments of cyber capabilities for water companies within Indiana.
  - Lack of understanding and knowledge of existing training for water company personnel.
  - No current regulations for cybersecurity for water companies.

- **Committee Deliverables**
  - Establish Water / Wastewater Cyber Contact with Indiana Department of Environmental Management (IDEM)
  - Cyber Risk Model (Plan)
  - Cyber Risk Tool
  - Training Plan
  - Cyber Security Plan Template for Senate Enrolled Act 362

- **Additional Notes**
  - [No Response]

- **References**
  - [No Response]

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. The Indiana American Water Works Association (AWWA) has provided training via the AWWA website.
    b. We created and ran the Indiana Crit-Ex exercises in 2015.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Small to mid-size water/wastewater utilities with internet access to their Supervisory Control and Data Acquisition (SCADA) systems.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Funding for cyber programs for small to mid-size water/wastewater utilities.
    b. Training on cybersecurity.
    c. Establishing the need for cybersecurity as a high priority compared to infrastructure upgrades.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. National Institute of Standards and Technology (NIST) cybersecurity standard, and the President's Executive Order on cybersecurity. Asset management plan and Cyber Security Plan through SEA 362.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Indiana Crit-Ex After Action Review

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. AWWA Articles/papers
    b. NIST

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Using the AWWA.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Annual cyber training.
    b. Practical cyber training at Muscatatuck.
    c. Federal and/or State financial support for cybersecurity improvements at small and mid-size water and wastewater facilities.
    d. State standards for cybersecurity.
    e. Established and automated cybersecurity risk model.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. Local cyber training
    b. Web-based training
    c. Local government support/awareness of the need for improved cyber

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. There are approximately 500 water companies in Indiana. There are currently no cybersecurity personnel.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. Crit-Ex; Cyber Gym; grow the corporate headquarters in Indiana. This creates the need for cybersecurity companies.

12. **What are your communication protocols in a cyber emergency?**
    a. Protocols vary by utility

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. Best practices should include risk-based templates for evaluating cyber risks based off of the NIST.

Deliverable: Cyber Contacts

Deliverable: Cyber Contact

General Information

1. **What is the deliverable?**
    a. The deliverable will be a cybersecurity contact list for water and wastewater organizations. The list will be in the form of a database that will be regularly updated with contacts specific to each organization's cybersecurity initiatives. This database will work in concert with existing databases that houses additional information for the individual organizations business structure. An added field will complement the focused contact information that exists and provides a direct contact for cyber-related information. The Safe Drinking Water Information System (SDWIS) contains information about public water systems managed by the Indiana Department of Environmental Management (IDEM) will be modified to include the added field for the 'SC' – SCADA Contact.

2. **What is the status of this deliverable?**
    a. In-progress; 50% 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 result will be a regularly updated database of cybersecurity contacts for the water / wastewater organizations in the state. The database will be managed and updated at regular intervals by the organizations through the existing update process by IDEM. This contact will alleviate specific focused information to the correct individual of each organization.

6. **What metric or measurement will be used to define success?**
    a. Database establishes a field for cybersecurity contacts. Cybersecurity contacts are updated by the individual organizations of medium and large operators.

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

8. **Who or what entities will benefit from the deliverable?**
    a. State organizations like IDEM, Department of Homeland Security (DHS), Indiana Utility Regulatory Commission (IURC), and Indiana State Police (ISP) will have the right contact for cybersecurity-related information sharing.
    b. Other industry organizations like Indiana's Water/Wastewater Agency Response Network (InWARN), AWWA, Indiana Rural Water, and Indiana Water Environment Association (IWEA) will also be able to information share using the database.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. IDEM will manage the database.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None at this time.

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

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

13. **What are the expected challenges to completing this deliverable?**
    a. Timely updates by the individual organizations will be required to supply the contact information.

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
Modify IDEM SDWIS Database to include new field	IDEM / Travis Goodwin	100	November 2017	IDEM completed database modifications.
Request organizations to submit 'SC'to IDEM for updates	IDEM	100	January 2018	Requests made to organizations. Awareness shared by partnering organizations INWarn, AWWA, Indiana Rural Water
Update database upon receipt of information	IDEM	20	2019	IDEM recently completed the regular update prior to inclusion of the 'SC'. Next regular update cycle anticipated to have better return.

Resources and Budget

15. Will staff be required to complete this deliverable? No.

a. No (see question 16)

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
Database maintenance	Database exists and team to complete. Additional field with minimal additional effort required to complete.	10 hours of database configuration.	2 minutes per field update (550 organizations)	IDEM operations		

Benefits and Risks

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

a. State organizations like IDEM, DHS, IURC, and ISP will have the right contact for cyber security- related information sharing.
b. Other industry organizations like InWARN, AWWA, Indiana Rural Water, IWEA will also be able to information share using the database.

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 expedite information sharing with the appropriate subject matter expert. Information could be critical information, education, and awareness specific to Indiana's water and wastewater sector.
b. Benefits also include supporting organizations will have the right individual to share information with and reach out for information that may support other organizations.

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

a. Cost avoidance by organizations creating their own contact list and time saved by having the information available to pertinent parties. Not completing the deliverable will continue the challenge of identifying the right contact for cybersecurity in the water and wastewater sector.

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

a. Database configuration and usage of the database available to supporting organizations as well as the state for expedited information. Success will be to have the 'SC' field completed for 95% of community water systems serving over a population of 3,301 or more people.

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

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. New York Department of Health, Division of Environmental Health Protection

Other Implementation Factors

---

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

a. Completion of the database is dependent on community water systems submitting contact information. Regular updates will be required for usefulness.

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

a. No

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

a. Ongoing support is already managed through IDEM and its current entry into the existing SDWIS database.

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

a. IDEM – Travis Goodwin and Brian Rockensuess

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All sectors could use for information sharing. A contact database for other sectors could be created where applicable

Communications

---

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

a. State organizations: IDEM, IDHS, IURC, and ISP.
b. Other industry organizations: InWARN, AWWA, Indiana Rural Water, IWEA

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

a. No
b. Critical contact information should not be shared. IDEM should manage contact information requests specific to critical infrastructure.
c. Reference Indiana Code (IC) 5-14-3, specifically as the disclosure relates to sections:
    i. IC 5-14-4(b)(19)(L)
    ii. IC 5-14-4(b)(8).

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

a. **[**No Response]

Evaluation Methodology

Objective 1: Indian Department of Environmental Management conduct modifications to Safe Drinking Water Information System to collect cybersecurity contact information for Indiana water and wastewater organizations by November 2017.

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: Indian Department of Environmental Management maintains a cybersecurity contact information for 95 percent of Indiana water organizations serving a population greater than 3,301 by December 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 – Year 2
☒ Quantifiable Measurement
☐ Other

Deliverable: Cyber Risk Model (Plan)

Deliverable: Cyber Risk Model (Plan)

General Information

1. **What is the deliverable?**
    a. The deliverable is a risk framework assessment tool for the industrial control system that uses the NIST Cybersecurity Framework and AWWA Cybersecurity tool that is end-user friendly. The tool should have the capability to be completed through a one-day onsite visit. The resulting tool could be modified by other working groups and organizations to fit specific needs that may not be found in the water/wastewater industrial control systems.

2. **What is the status of this deliverable?**
    a. The risk framework has been established as a draft document. The effort has been put on hold while the cybersecurity risk template is prepared for SEA 362.

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The result will be a standard method for organizations to perform a risk assessment that is user friendly and the capability to conduct onsite visits. Currently, organizations are using various methods and standards to perform assessments. This deliverable will be consistent with the NIST framework and industry-specific AWWA cybersecurity tools.

6. **What metric or measurement will be used to define success?**
    a. Testing will be performed by conducting two risk assessments (RA) on Indiana water companies. Success will be the refinement of the templated assessment to enable completion of an assessment within a day for organizations with varying business structures and size.

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

8. **Who or what entities will benefit from the deliverable?**
    a. Water and wastewater entities will benefit by having a mitigation report and areas of improvement identified. Entities will be able to demonstrate improvement by using a consistent tool for measuring improvements to their cyber posture. Other entities with industrial control systems will benefit by using the template tailored specifically to their organizations.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Department of Homeland Security has an assessment through the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) that provides similar results.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. We believe other groups with similar initiatives could share the product outcome for performing their own assessments within their groups.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Finance Authority (IFA) to provide resources in order for entities to complete assessments.
    b. American Water Works Association has expressed an interest in Indiana's initiatives focusing on cybersecurity for the industry.
    c. Academia (IUPUI / Purdue University) in the development of the assessment and resources to perform assessments.
    d. DHS ICS-CERT would be beneficial to come alongside the working group to share resources and development tools.

12. Who should be main lead of this deliverable?

a. Professor Connie Justice

13. What are the expected challenges to completing this deliverable?

a. Challenges are the resources to develop the assessment template. Once developed additional resources to perform the assessments: 500 + entities * 8 hours = 4,000 contact hours.

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
Questionnaire	Justice / Water and Wastewater Group	100	April 2018	
Risk Assessment Documentation	Justice	100	April 2018	
Risk Assessment Onsite Beta Test	Justice	100	April 2018	Risk Assessment Scheduled in April 2018 with Lewisville, IN Water. Risk Assessment scheduled with Speedway, IN Waste Water in April 2018.
Risk Assessment Report	Justice	0	September 2018	
Review Assessment Results with the Water and Wastewater Group	Water and Wastewater Group	0	October 2018	
Rewrite Questionnaire/Report if needed	Water and Wastewater Group	0	December 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
Water and Wastewater Council Group	Expertise	0	0	N/A	N/A	
Graduate Students	Professional Education	0	0	N/A	N/A	
Dr. Justice	Expertise	0	0	N/A	N/A	
Dr. Kevin Morley, AWWA	Expertise	0	0	N/A	N/A	
Lewisville Water	Expertise	0	0	N/A	N/A	
Speedway Waste Water	Expertise	0	0	N/A	N/A	

Benefits and Risks

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

a. The State of Indiana and AWWA risk assessment model for water and wastewater utilities. Allows a state-wide standard and measurement to assist each individual water and wastewater utility with measuring their risks and the State with calculating of state-wide risks.

b. Regularly conducted risk assessments close cybersecurity vulnerabilities and mitigate before the vulnerabilities are compromised. Therefore, allowing the sector to understand their cybersecurity posture.

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

a. Along with the action plan for each utility, the risk model will allow the water and wastewater companies to reduce the risk for their utility and will thus reduce risk to the State of Indiana overall.

b. The risk assessments allow for determination of a baseline security measure that can show improvement with additional risk assessment results. More importantly, the risk assessment will identify chinks in the armor of employee security education, training, and awareness (SETA). This will allow a proper SETA program to be initiated and maintained. Additionally, the risk assessment allows for the sector to prioritize the most sensitive areas of cybersecurity that need attention and investment.
c. We are unable to estimate the costs at this time but will be in a better position after utilities have completed risk assessments.

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

a. If water and wastewater infrastructure is not protected, there could be a serious threat to the safety of the water supply and wastewater could breach into homes of Indiana citizens. Executive Order 13636 - Improving Critical Infrastructure Cybersecurity states that "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."

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

a. The baseline is an initial risk assessment score with mitigations to be implemented. Success is defined as successful completion of risk assessment with a score and the implementation of at least one mitigation recommendation.

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

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. The AWWA has developed a cyber self-assessment tool that is available to any company nationwide that can be used by any water/wastewater utility. The AWWA has expressed interest in the Indiana cyber model tool that can be used across the country and will provide funding up to $40,000. We will describe the tool in our second deliverable

Other Implementation Factors

---

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

a. The lack of volunteers' time to accomplish initial tasks.

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

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. Water/Wastewater cybersecurity committee will work with the AIM committee, IDEM, and the IFA to ensure the template meets their requirements; and approved by IDEM and IFA as acceptable in order to meet State Law SEA 362

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

a. To support this deliverable in the future, a tool will need to be created to simplify the risk assessment for the sector client.

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

a. AWWA, IDEM, AIM-Rhonda Cook, Stephanie Yeager; Chetrice Mosley, Dewand Neely, and Brian Langley.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. This risk assessment can be used by all sectors

Communications

---

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

a. Indiana water and wastewater companies, AWWA, IOT, IDHS, IDEM

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

a. Yes

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

a. Defer to Chetrice Mosley

Evaluation Methodology

Objective 1: IECC Water & Wastewater Committee and partners develop Cyber Plan Template for Indiana water/wastewater companies by December 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 Water & Wastewater Committee and partners distribute Cyber Plan Template to twenty-five percent of Indiana water/wastewater companies by March 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: Risk Tool

Deliverable: Risk Tool

General Information

1. **What is the deliverable?**
    a. The deliverable is a risk framework assessment tool for the industrial control system that uses the NIST Cybersecurity Framework and AWWA Cybersecurity tool that is end-user friendly. The tool should have the capability to be completed through a one-day onsite visit. The resulting tool could be modified by other working groups and organizations to fit specific needs that may not be found in the water/wastewater industrial control systems.

2. **What is the status of this deliverable?**
    a. Not Started

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The result will be a standard method for organizations to perform a risk assessment that is user friendly and the capability to conduct onsite visits. Currently organizations are using various methods and standards to perform assessments. This deliverable will be consistent with the NIST framework and industry specific AWWA (American Water Works Association) cybersecurity tools.

6. **What metric or measurement will be used to define success?**
    a. Testing will be performed by conducting 2 risk assessments on Indiana water companies. Success will be the refinement of the template assessment to enable completion of an assessment within a day for organizations with varying business structures and size.

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

8. **Who or what entities will benefit from the deliverable?**
    a. Water and wastewater entities will benefit by having a mitigation report and areas of improvement identified. Entities will be able to demonstrate improvement by using a consistent tool for measuring improvements to their cyber posture. Other entities with industrial control systems will benefit by using the template tailored specific to their organizations.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Department of Homeland Security has an assessment through ICS-CERT that provides similar results.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. We believe other groups with similar initiatives could share the product outcome for performing their own assessments within their groups.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Finance Authority to provide resources in order for entities to complete assessments.
    b. American Water Works Association has expressed an interest in Indiana's initiatives focusing on cybersecurity for the industry.
    c. Academia (IUPUI / Purdue University) in the development of the assessment and resources to perform assessments.
    d. DHS ICS-CERT would be beneficial to come alongside the working group to share resources and development tools.

12. **Who should be main lead of this deliverable?**
    a. Professor Connie Justice

13. **What are the expected challenges to completing this deliverable?**
    a. Challenges are the resources to develop the assessment template. Once developed, additional resources to perform the assessments (500 + entities * 8 hours = 4000 contact hours).

Implementation Plan

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

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review and modify initial documents for accuracy	TBD	0	TBD based on funding	
Review with IOT to establish technical standards	TBD		TBD based on funding	
Establish detailed project plan	TBD		TBD based on funding	
Questionnaire	C. Justice/Water and Wastewater Group	0	TBD on project plan	NIST CSF/AWWA
Review Questionnaire	Water and Wastewater Group	0	TBD on project plan	
Risk Assessment Scoring Matrix	C. Justice	0	TBD on project plan	
Review of Risk Assessment Scoring Matrix	Water and Wastewater Group	0	TBD on project plan	Output score and where entity ranks in relation to others. Mitigation recommendations. Training needed
Risk Assessment Program Created	C. Justice /Programming Staff	0	TBD on project plan	Computer, tablet, mobile devices
Test Risk Assessment Program	C. Justice /Programming Staff	0	TBD on project plan	
Conduct Risk Assessment Sector	C. Justice/Water and Wastewater Group	0	TBD on project plan	

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
Dr. Justice	Risk Assessment Content	0	0		N/A	
Programmers	Programming expertise	80,000.00	TBD	State/AWWA	N/A	
IoT	Expertise	0	TBD		N/A	

Benefits and Risks

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

a. Speed consistency, ease of use, the ability of water/waste water companies to conduct without third party support.
b. The ability to automate the risk assessment will allow for ease of use and automation of risk assessment results and the uploading of the data to a repository where the data can be referenced and used for baseline data for company and Indiana can use the data for measuring the effectiveness of the program.

18. How will this deliverable reduce the cybersecurity risk or impact?

a. More utilization since local water or wastewater utilities can use the tool to establish the utilities cyber risk profile.

19. What is the estimated costs associated with that risk reduction?

a. Estimated costs associated = 400 water companies x 16 hours x 2 people to conduct assessment onsite. Having an electronic tool will allow many, if not all, of the utilities to prepare the risk assessment themselves, thus reducing the estimated hours to conduct a manual risk assessment.

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

a. If water and wastewater infrastructure is not protected, there could be a serious threat to the safety of the water supply and wastewater could breach into homes of Indiana citizens. Executive Order 13636 - Improving Critical Infrastructure Cybersecurity states that "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."

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

a. 80% will have conducted the assessment within 24 months of tool deployment.

22. 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

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

a. No

Other Implementation Factors

---

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

a. Program scope creep.
b. Problems with programming features of risk assessment software.

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

a. No

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

a. Support of modifying model to changes of NIST model
b. IOT support to modify the tool

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

a. IDEM, Chetrice Mosley, Dewand Neely, and Brian Langley

28. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. This risk assessment can be used by all sectors

Communications

---

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

a. Indiana water and wastewater companies, AWWA, IOT, IDHS, IDEM

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

a. Yes

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

a. Defer to Chetrice Mosley

Evaluation Methodology

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

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Objective 2: Eight percent of Indiana water and wastewater companies will have used cyber assessment risk tool within 24 months of deployment.

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Deliverable: Training Plan

Deliverable: Training Plan

General Information

1. **What is the deliverable?**
    a. The main deliverable is a Training Plan, consisting of three main components:
        i. An assessment survey that identifies the skills required by each actor within the system to fulfill their responsibilities utilizing the best practices of cybersecurity. Each skill will be mapped to a requirement for the industry, in the case of the Water Sector, the AWWA interpretation of the NIST standards. The skills themselves will be mapped against sources where the training required to satisfy the requirement can be obtained. A weighting will be assigned to each role/skill providing a scorecard of the skills gap.
        ii. A method for the reporting of assessment results into a (State) database to allow for the guidance of academia and course providers in the development and refinement of coursework, i.e., a managed database of training statistics.
        iii. A glossary of common terms will be developed to allow for cross sector utilization of the training plan. This will allow an organization to view cybersecurity holistically across their organization.

2. **What is the status of this deliverable?**
    a. Not Started

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. The desired outcome of the Training Plan will be a significant reduction in the skills gap within Industrial Control System providers, Water Facility OT/IT personnel and associated admin and support staff.

6. **What metric or measurement will be used to define success?**
   a. The Training Plan will have as a central aspect a skills/responsibilities matrix with which an organization can map skills required by role and the training required to satisfy that requirement. Using the initial assessment as their baseline, they will able to quantify both their absolute gap and their growth, or lack thereof over each period.

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

8. **Who or what entities will benefit from the deliverable?**
   a. The completed and executed training plan will benefit each water entity that utilizes it to quantify their skills gap and then measure growth in developing critical cybersecurity skills in a prioritized manner.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. TBD

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. This is to be established. I will work with Ms. Mosley to define other sectors and/or committees that might have an interest in collaborating on this effort.

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

12. Who should be main lead of this deliverable?

a. Cliff Campbell

13. What are the expected challenges to completing this deliverable?

a. Time and resources. This will require a significant effort in research and implementation.

Implementation Plan

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

a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Develop project plan	Training Working Group/Water and Wastewater Committee	0	TBD based on funding	
Develop roles by job function	Training Working Group/Water and Wastewater Committee			
Develop framework of skills required of each role within entity	Training Working Group/Water and Wastewater Committee	0	TBD on project plan	
Map skills to appropriate Standard	Training Working Group/Water and Wastewater Committee	0		
Cross reference skills to available training	Training Working Group/Water and Wastewater Committee	0		
Develop skills assessment scoring matrix	Training Working Group/Water and Wastewater Committee	0	TBD on project plan	
Skills Assessment Tool Created	Training Working Group/Water and Wastewater Committee	0	TBD on project plan	Computer, tablet, mobile devices
Validate Skill Assessment Tool	Training Working Group/Water and Wastewater Committee	0	TBD on project plan	

Coordinate with industry associations for distribution and collection of survey	Training Working Group/Water and Wastewater Committee	0	TBD on project plan	
Determine proper authority to host statewide database of skills	Training Working Group/Water and Wastewater Committee			
Determine relevant parameters to include in database	Training Working Group/Water and Wastewater Committee			
Create Database	Training Working Group/Water and Wastewater Committee			
Coordinate cross sector team to develop common glossary	Training Working Group/Water and Wastewater Committee			
Develop Common Glossary	Training Working Group/Water and Wastewater Committee			

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
[No Response]					

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

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
[No Response]						

Benefits and Risks

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

a. The State of Indiana and AWWA skills assessment model for water and wastewater utilities. Allows a state-wide standard and measurement to assist each individual water and wastewater utility with measuring their skills gap and the state with measurement of state-wide training needs.
b. Regularly conducted skills assessments close cybersecurity training gaps and mitigate before the vulnerabilities are compromised. Therefore, allowing the sector to understand their cybersecurity skills gap.

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

a. Along with an action plan for each utility, the risk model will allow the water and wastewater companies to reduce the risk for their utility and will thus reduce risk to the State of Indiana overall.
b. The skills assessments allow for determination of a baseline security measure that can show improvement with additional risk assessment results. More important, the risk assessment will identify chinks in the armor of employee security education, training, and awareness (SETA) so that a proper SETA program can be initiated and maintained. Additionally, the risk assessment allows the water/wastewater sector to prioritize the most sensitive areas of cybersecurity that need attention and investment.

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

a. Along with an action plan for each utility, the risk model will allow the water and wastewater companies to reduce the risk for their utility and will thus reduce risk to the State of Indiana overall.
b. The risk assessments allow for determination of a baseline security measure that can show improvement with additional risk assessment results. More important, the risk assessment will identify chinks in the armor of employee security education, training, and awareness (SETA) so that a proper SETA program can be initiated and maintained. Additionally, the risk assessment allows the sector to prioritize the most sensitive areas of cybersecurity that need attention and investment.

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

a. Using the initial assessment as their baseline, they will able to quantify both their absolute gap and their growth, or lack thereof over each period. At a higher level, success can be evaluated on both a utilization percentage, as well as qualitative
b. The baseline is an initial risk assessment score with mitigations to be implemented. Success is defined as successful completion of risk assessment with a score and the implementation of at least one mitigation recommendation.

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

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. The lack of volunteers' time to accomplish initial tasks.

24. **Does this deliverable require a change from a regulatory/policy standpoint**?
    a. Yes
        i. Water/Wastewater cybersecurity committee will work with the AIM committee, IDEM, and the IFA to ensure the template meets their requirements; and approved by IDEM and IFA as acceptable in order to meet State Law SEA 362

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. [No Response]

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. [No Response]

27. **Can this deliverable be used by other sectors**?
    a. Yes
    b. **If Yes, please list sectors**
        i. This risk assessment can be used by all sectors

Communications

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. Indiana water and wastewater companies, AWWA, IOT, IDHS, IDEM

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

30. **What are other public relations and/or marketing considerations to be noted?**
    a. [No Response]

Evaluation Methodology

Objective 1: Water/Wastewater Committee develop a training plan within three months of securing funding.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

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

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Deliverable: Cyber Plan Template

Deliverable: Cyber Plan Template

General Information

1. **What is the deliverable?**
    a. With the passage of SEA 362, water and wastewater utilities are required to have a cybersecurity plan. There is not an industry standard for cybersecurity plans for water or wastewater utilities. The NIST framework has the necessary items to establish one, but the framework is large and confusing for most water and wastewater utility personnel. There is a need for a simple and straightforward cybersecurity plan template that can be used to assist utilities in the establishment of their specific plan in order to comply with SEA 362.

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 result will be a standard method for utilities to establish and maintain a cybersecurity plan and program. This will provide for a significantly safer water delivery system for the State of Indiana.
    b. The template is in development at this time. This draft template is currently "Open for Comments". It will continue this status for the next 60+ days. The current draft version of the template is contained in this plan's Supporting Documentation.

6. **What metric or measurement will be used to define success?**
    a. Validation by the water and wastewater committee, with an approval vote. Review and certification of IDHS, IDE, IFS, and IOT.

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

8. **Who or what entities will benefit from the deliverable?**
    a. Water and wastewater utilities and the citizens of Indiana.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. [No Response]

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Local government.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Finance Authority will need to certify the plan template.
    b. Indiana Department of Environment Management will need to certify the plan template.

12. **Who should be main lead of this deliverable?**
    a. John Lucas, Chair of the Water/Wastewater committee

13. **What are the expected challenges to completing this deliverable?**
    a. Getting the needed reviews in order to get the cybersecurity plan template completed.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Cyber Security Plan Template	Justice/Water and Wastewater Group	100%	October 2018	
Review of cyber security plan template by IDEM, IFS, AIM, and external partners	John Lucas	25%	December 2018	
Finalized cyber security plan template for distribution by IDEM.	IDEM, IFS, IDHS, Water and Wastewater committee	0	April 2019	

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
Water and Wastewater Council Group	Expertise	0	0	N/A	N/A	
IDEM	Professional Education	0	0	N/A	N/A	
IFS	Expertise	0	0	N/A	N/A	
IDHS	Expertise	0	0	N/A	N/A	

Benefits and Risks

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

a. This will be the standard for all water/wastewater companies to establish a cybersecurity plan, and improve the cybersecurity of the water and wastewater utilities for the residents of the State of Indiana.

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

a. This will establish a baseline level of cybersecurity for all Indiana water & wastewater utilities. This plan will improve the utilities to protect utility assets and respond to a cyberattack much more quickly. This will reduce the risk to the residents of the state, and reduce the impact of an attack.

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

a. Water and Wastewater utilities will not have a baseline for establishing a security posture, and will be unable to meet the requirements of SEA 362.

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

a. Establishment of a cybersecurity plan template, and the usage of this template to better secure water and wastewater utilities in Indiana.

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

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. No
b. **If Yes, please list states/jurisdictions**

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

a. The short timeframe of this effort will put stress on the individuals who are writing the plan, and on the agencies who will be responsible for reviewing and implementing the plan.

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

a. Yes
    i. The water/wastewater cybersecurity committee will work with the AIM committee, IDEM, and the IFA to ensure the template meets their requirements; and approved by IDEM and IFA as acceptable in order to meet State Law SEA 362.

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

a. This template will need to be updated regularly as cybersecurity standards and methods like the NIST standard change.

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

a. IDEM, AIM-Rhonda Cook, Stephanie Yeager; Chetrice Mosley, Dewand Neely, and Brian Langley, IFS

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. This template could be used with modifications by other sectors.

Communications

---

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

a. Indiana water and waste water companies, AWWA, IoT, IDHS, IDEM, IFS

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

a. Yes

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

a. [No Response]

Evaluation Methodology

Objective 1: IECC Water and Wastewater Committee develop a Cyber Plan Template for Indiana water/wastewater companies by April 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

Objective 2: IECC Water & Wastewater Committee and partners distribute Cyber Plan Template to 50 percent of Indiana water/wastewater companies by October 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.

- IECC DRAFT Water and Wastewater Cybersecurity Plan Template

IECC Water and Wastewater Committee

Cybersecurity Plan Template

September 2018

WATER AND WASTEWATER CYBERSECURITY PLAN TEMPLATE

i. VERSION HISTORY

Date	Version	Description
05/29/2018	0.1	Initial Draft
6/7/2018	0.2	Modifications – Connie Justice
6/11/2018	0.3	Modifications- Sondhi Solutions
6/11/2018	0.4	Modifications – Connie Justice
6/17/2018	0.5	Modifications- Sondhi Solutions
06/20/2018	1.0	Second Draft – Connie Justice
6/21/2018	1.1	Modifications – Connie Justice and John Lucas
6/29/2018	2.0	Third Draft – Connie Justice
7/10/2018	2.1	Modifications-Connie Justice
7/20/2018	2.2	Modifications-Connie Justice
7/30/2018	2.3	Modifications – Connie Justice
8/15/2018	2.4	Modifications – Connie Justice
8/26/2018	3.0	Fourth Draft – Connie Justice
9/6/2018	3.1	Modifications – Connie Justice, John Lucas, Steve Berube, Jaimie Foreman, Jon Weirick

ii. Contributors and Acknowledgements

This cyber security template was developed by the Water / Wastewater committee of the Indiana Executive Cyber Security Committee of the State of Indiana. This committee is a committee of business, government, and regulatory members from across the State of Indiana.

iii. Important Terms

Term	Definition

iv. Table of Contents

i. Version History 2
ii. Contributors and Acknowledgements 3
iii. Important Terms 3
iv. Table of Contents 4
Introduction 1
Acronym List 1
Cybersecurity Plan Checklist 2
1 Identify 2
Return to Checklist 3
2 Protect 4
Return to Checklist 5
3 Detect 5
Return to Checklist 6
4 Respond 7
Return to Checklist 8
5 Recover 8
Return to Checklist 9
Exhibit 1: Data Classification Template 10
6 Exhibit 2: Critical Asset Inventory Per Facility 11
7 Exhibit 3: Policy Examples 12
8 Exhibit 4: Water Waste Water Risk Assessment (To Be Delivered) 13
9 Exhibit 5: Employee Training and Awareness 14
10 Exhibit 6: Securing Network and Cloud 15
11 Exhibit 7: Maintenance Life Cycle Process 17
12 Exhibit 8: Emergency Response Plan (ERP) 18
13 Exhibit 9: Contact List 19
14 Exhibit 10: After Action Report 20

INTRODUCTION

This document is a checklist of recommendations for maintaining the overall Cybersecurity posture of a Water or Wastewater Treatment operation. To be effective, each entity must ensure the cooperation of its IT Department, the Water and Wastewater Operations, and a Cybersecurity partner (if additional expertise in this area is required). Having a plan is only the first step. At least twice a year, you should verify that people, systems and software continue to align with your cybersecurity plan. Create a ledger to ensure you've covered identified recommendations. The guide is based on NIST cyber security framework and the EPA Incident Action Checklist – Cybersecurity. This document has been established in order for Water utilities to become compliant with Indiana Senate bill 362.

HOW TO USE THIS GUIDE

The document should be followed in the creation of policies, processes, and programs and verified by a Cybersecurity lead and clearly documented as part of the regularly executed Cybersecurity maintenance routine. A secure document management repository should be used to maintain and publish all documentation revisions.

ACRONYM LIST

IT	Information Technology
EPA	Environmental Protection Agency
NIST	National Institute of Standards and Technology
CSF	Cybersecurity Framework
AWWA	American Water Works Association
US-CERT	US-Computer Emergency Readiness Team
FFIEC	Federal Financial Institutions Examination Council
IDS	Intrusion detection system
TCP/IP	Transmission Control Protocol/Internet Protocol,
ICS	Industrial controls system
NIST SP	NIST Special Publication
ERP	Emergency response plan
NCCIC	National Cybersecurity & Communications Integration Center
INWARN	
IDHS	Indiana Department of Homeland Security
ISAC	Water Information Sharing and Analysis Center (WaterISAC)
WATER-ISAC	Water Information Sharing and Analysis Center (WaterISAC)

AAR	After action report
IP	Improvement plan
SOX	Sarbanes Oxley
HR	Human resources
PII	Personally identifiable information
HIPAA	The Health Insurance Portability and Accountability Act
SCADA	Supervisory control and data acquisition
CSRC	Computer Security Resource Center (CSRC)
SANS	SANS Institute was established in 1989 as a cooperative research and education organization
DMZ	Demilitarized zone
NMS	Network monitoring system
IPSEC	Internet Protocol Security
AES	Advanced Encryption Standard
WPA2	Wi-Fi Protected Access II
DHS	Department of Homeland Security
POC	Point of Contact

Cybersecurity Plan Checklist

Identify

- [ ] Identify Organization Security Lead
- [ ] Classify data
- [ ] Identify assets
- [ ] Security policies
- [ ] Risk Assessment
- [ ] Risk Management Strategy

Protect

- [ ] Employee Training and Awareness
- [ ] Access Control
- [ ] Securing Network and Cloud
- [ ] Authentication Policy
- [ ] Data Security
- [ ] Information Protection
- [ ] Maintenance
- [ ] Protective Technology
- [ ] Physical Access

Detect

- [ ] Anomalies and Events
- [ ] Continuous Monitoring
- [ ] Detection Processes

Respond

- [ ] Response Planning
- [ ] Respond Communications
- [ ] Analysis
- [ ] Mitigation
- [ ] Respond Improvements

Recover

- [ ] Recovery Planning
- [ ] Recovery Improvements
- [ ] Recovery Communications

1 IDENTIFY

When they happen, cybersecurity events are very stressful. This is not a time when you want to guess about who to call or where to find a serial number for an affected device. To help prepare for an event, it is important to create and maintain inventories of your assets. Knowing how those assets connect and work together is also very important. Having a list of contacts will ensure you have access to people and organizations in the event of an emergency. Building and maintaining an Information Technology Asset Inventory ensures you have critical information on your organization's technology items as they come in and out of their life cycle. Give each asset a unique code and label when entered into the inventory as they come into operation. Review the inventory at least annually and note items that are nearing "end of life" and plan to retire or replace them. Appendix A: IT Asset Inventory has a template to help you get started.

1.1 ORGANIZATION SECURITY LEAD

a. Identify an organization security lead
b. Identify emergency response team

1.2 ASSET MANAGEMENT

a. Identify mission critical data assets and classify data assets in order of importance. Identify personnel responsible for data asset/s.
b. See Exhibit 1 for data classification template
c. Identify mission critical assets
    a. Identify Mission Critical Technology Assets
        1. Applications (email applications, web browsers, productivity applications)
        2. Data (What storage devices data is stored on: hard drives, portable media, off site data backups)
        3. Servers (hardware devices that can host applications, or other virtual servers)
        4. Workstations/HMI/PLC (Systems that run SCADA software, Systems that run Business Software)
        5. Field devices (Laptops, Tablets, Cell Phones)
        6. Communications and network equipment (router, firewall, voice system)

Note: See Exhibit 2 for asset identification table template.

1.3 BUSINESS ENVIRONMENT AND GOVERNANCE

a. Governance framework is used to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.
b. Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.
c. Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.
d. Security Policies and Procedures Exhibit 3

1.4 Risk Assessment

1.4.1 Conduct a Risk Assessment

a. Execute a cybersecurity risk assessment to identify vulnerabilities in business and industrial control mission critical systems using the NIST CSF/AWWA tool (Link to Indiana Water/Wastewater Risk Model will be added).
b. Create action plan to mitigate significant vulnerabilities identified in risk assessment, and act on the mitigation plan.
    a. Create an action plan that prioritizes actions needed to mitigate risk.
    b. Prioritize the implementation of protective measures
    c. Low hanging fruit-Optimize your budget in relation to identified risks.

1.4.2 Risk Management Strategy

a. A security program established to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks.
b. Risk management is the process of identifying what information requires what level of protection and then implementing the proper level of protection and subsequently monitoring the protection.
   The basic risk strategy is:
    a. Identify basic information stored and used in the business
    b. Determine the classification or value of the information
    c. Inventory the assets in the business
c. Understand what threats and vulnerabilities exists in the business

1.5 *Links for IDENTIFY section*

a. US-CERT's Protect Your Workplace Posters & Brochure: http://www.us-cert.gov/reading_room/distributable.html
b. Socializing Securely: Using Social Networking Services: http://www.us-cert.gov/reading_room/safe_social_networking.pdf
c. Governing for Enterprise Security: http://www.cert.org/governance/
d. FFIEC Handbook Definition of Reputation Risk: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk- management/reputation-risk.aspx
e. What Businesses can do to help with cyber security: http://www.staysafeonline.org/sites/default/files/resource_documents/What%20Businesses%20Can%20Do%202011%20Final_0.pdf

Return to Checklist

2 PROTECT

The next step in your cybersecurity plan should be to determine what protections to put in place. This helps to limit exposure and limit damage in the event of an attack. Protections can include the following:

a. A way to control access to the IT assets you identified in Step 1.
b. A plan to provide cybersecurity awareness and training to your staff
c. A method to determine how to keep data, networks and systems secure
d. A plan to make sure systems are up-to-date with patches or if you can't patch systems then have appropriate controls to make sure systems are not modified (i.e. Scada systems with whitelisting).
e. A decision to use protective technologies to help prevent threats if appropriate

2.1 EMPLOYEE TRAINING AND AWARENESS

Employees should be trained and be aware of cybersecurity issues and situations that can compromise the business and ruin the company's reputation. See Exhibit 5 for training and awareness guidelines.

2.2 ACCESS CONTROL

2.2.1 SECURING NETWORK AND CLOUD

The network infrastructure is the backbone for defenses against internal and external malicious programs and nefarious persons. Layered protection and various devices are the key to protecting internal networks from these bad actors. Cloud services are becoming common place to conduct business. Ensure secure communications and multifactor authentication are setup between the business and cloud providers. See Exhibit 6 for example template of securing network and cloud.

2.2.2 IMPLEMENT A RIGOROUS USER AUTHENTICATION POLICY

a. Multifactor-authentication should be used wherever possible.
b. Use a passphrase instead of a password. A passphrase is a phrase constructed of multiple words. An example would be: "sunwalkraindrive". A passphrase constructed of 4 words (sun + walk + rain + drive) is easy to remember but hard to guess. It is not recommended that users change their passwords because of the general predictability in which users change specific characters.
c. Use unique passphrases for separate confidential accounts.

2.2.3 DATA SECURITY

In addition to understanding data classification, it is important to protect business data. Sensitive business data should be encrypted on storage medium and data should be encrypted in transit from end to end communications. The key elements to secure data are:

a. Data at rest is encrypted
b. Data in transit is encrypted
c. Logging in place to protect against data leaks
d. Systems in place to ensure integrity of data

2.3 Information Protection Processes and Procedures

Data should also be protected by proper backups and testing. Additionally, proper destruction of data is very important, as well as having an incident response, disaster recovery, and business continuity plan in place.

a. Backup and restore of data are tested
b. Data destruction process is in place
c. Incident response, disaster recovery, and business continuity plans are in place and managed.

2.4 Maintenance

Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity. See Exhibit 7 for the asset management process.

2.5 Protective Technology

a. Storage media management and disposal program established to ensure that any sensitive data/software is used appropriately and is removed prior to media disposal (including approved policies and procedures).
b. Centralized logging system including policies and procedures to collect, analyze and report to management.
c. SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.
d. Program for hardening servers, workstations, routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).

2.6 Physical Access

a. Physical access to facilities and areas where operational equipment is running should be limited to staff who require the access to perform their job. A more liberal policy on access control is not best practice and would inevitably provide access to individuals who accidently or purposefully create problems with the environment.
b. Physical Security should be implemented to ensure access is given to areas with operational or IT systems only to those personnel who need access to these areas to perform their job duties.
c. No access to the internet should be permitted to industrial control systems unless absolutely required. If required, a web content filter should be used to limit the access to the system based on a policy.

Return to Checklist

3 Detect

Organizations must implement the appropriate measures to quickly identify cybersecurity events. The adoption of continuous monitoring solutions that detect anomalous activity and other threats to operational continuity is required to comply with this function. Organizations should have network

visibility in order to anticipate a cyber incident; which should be included in your current cybersecurity plan.

3.1 Anomalies and Events

a. An intrusion detection system (IDS) should be implemented to identify malicious activity. IDS systems are designed to watch for signatures of malicious traffic, or to recognize anomalies in the underlying TCPIP communications. If anything falls outside of the normal patterns for how these protocols work, the IDS will send an alert to the administrator for the system who can then act upon the alert by implementing a firewall rule to block the offensive traffic.
b. Security Continuous Monitoring. A basic logging server should be deployed to aggregate log data from different devices to correlate alerts and notify the administrator when certain thresholds have been met (e.g. 3 or more failed logins for an account).

3.2 Security Continuous Monitoring

a. Monitoring for unauthorized personnel, connections, devices, and software is performed
b. Active monitoring for adversarial system penetration
c. Intrusion prevention systems should be configured to monitor for suspicious activity crossing your network perimeter
d. If you use a web filtering system, employees should have clear knowledge of how and why their web activities will be monitored, and what types of sites are deemed unacceptable by your policy.
e. Identification of security deficiencies in existing hardware and software.

3.3 Detection Processes

a. Continuous monitoring is a very effective way to analyze and prevent cyber incidents in ICS networks. Use intrusion detection systems, intrusion prevention systems and file integrity checkers to spot intrusions and verify web content.
b. Register for cybersecurity alerts and advisories from water sector and government partners to be aware of new vulnerabilities and threats (two sources of cybersecurity alerts are WaterISAC, which has a basic membership that is free, and ICS-CERT (https://ics-cert.us-cert.gov/alerts)).
c. Ensure the ICS network is separated from the public network. Additionally, the business network should be segmented from the ICS network using industry best practices (NIST SP 800-82 section 5).
d. Restrict internet access to industrial control systems unless there is a critical need.
e. System acceptance standards including data validation (input/output), message authenticity, and data integrity established to detect information corruption during processing.

Return to Checklist

4 RESPOND

a. Should a cyber incident occur, organizations must have the ability to contain the impact. To comply, your organization should utilize your response plan which should include processes such as:
    i. define communication lines among the appropriate parties
    ii. collect and analyze information about the event
    iii. perform required activities to eradicate the incident
    iv. incorporate lessons learned into revised response strategies.
b. The Emergency Response Plan (ERP) should be referenced and adhered to in the event of a Cybersecurity incident. The Emergency Response Team should be comprised of essential personnel that should be contacted, followed by the contacts listed in the Emergency Response Plan including all other utility personnel and media outlets as necessary. NCCIC can also assist with critical system response and recovery (888-282-0870 or NCCIC@hq.dhs.gov)

4.1 RESPONSE PLANNING

A security and response program should be established to ensure staff is aware of security policies and incident response/notification procedures. See Exhibit 8 for ERP steps.

4.2 COMMUNICATIONS

Contacts

a. Have ready access to a list of primary and backup contacts for personnel or entities (vendors, government agencies, etc.) responsible for the operation and maintenance of each critical system.
b. Next, identify priority points of contact for reporting a cyber incident and requesting assistance with response and recovery. Include any state resources that may be available such as Indiana State Police, Indiana National Guard Cyber Division or mutual aid programs (INWARN), as well as the Indiana Department of Homeland Security to assist with an attack and any other contact information needed. Exhibit 9: Emergency Contacts has a template to help organize necessary contacts.

4.3 ANALYSIS

a. Investigate notifications from detection systems
b. Understand incidents
c. Incidents are categorized appropriately per response plans
d. A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.

4.4 MITIGATION

a. Contain incidents
b. Mitigate incidents
c. Newly identified vulnerabilities are mitigated or documented as accepted risks

4.5 Improvements

a. Incorporate lessons learned from response plans
b. Update response plans

4.6 Contacts

4.6.1 Assess the damage to utility systems and any disruption to operations.

A checklist should be created for use in the Emergency Response Plan to verify functionality for critical business services and their supporting infrastructure. Any affected services should be documented and relayed to the administrator of the Emergency Response Plan. The administrator of the Emergency Response Plan should also document any reports of suspicious communications before or during the incident. The documentation should include date and time that information was reported.

4.6.2 Forensics Image

a. A forensic image should be taken of the impacted systems and transferred to other secure media that is not connected to a network. If possible, the original systems that were affected should be disconnected from the network and not powered down or rebooted.
b. After containment and a forensic image has been captured and the original system has been taken off the network and preserved for evidence, restore the system function to a new system from the last known good backup before the infection occurred.
c. Never work on the original evidence when responding to a Cybersecurity incident. This will ensure the integrity of the original evidence.

4.6.3 Lessons Learned

a. A Lessons Learned session should be conducted after an incident has been resolved. Each problem, it's perceived cause, and what should have been done differently should be discussed.
a. Positive feedback should also be discussed to show what went right during the response.
b. Submit the incident to WaterISAC and Indiana AWWA. The online WaterISAC incident report form can be found at https://www.waterisac.org/report-incident or a call can be placed at 866-H2O-ISAC. Additionally, report incident to Indiana AWWA.

Return to Checklist

5 Recover

5.1 Recovery Planning

Policies and procedures for system instantiation/deployment should be established to ensure business continuity.

5.2 Improvements

Develop a lessons learned document and/or an after action report (AAR) to document utility response activities, successes, and areas for improvement. Create an improvement plan (IP) based on your AAR and use the IP to update your vulnerability assessment, ERP and contingency plans. See Exhibit 10 for an example AAR report.

5.3 Communications

a. Organizations must develop and implement effective activities to restore any capabilities or services that were impaired due to a cybersecurity event. Organizations must have a recovery plan in place, be able to coordinate restoration activities with external parties and incorporate lessons learned into updated recovery strategy. Defining a prioritized list of action points which can be used to undertake recovery activity is critical for a timely recovery.
b. The organizations recovery plan should address damage to reputation from data breaches, criminal organizations, inappropriate employee actions.
c. Mission critical processes should be documented in the Emergency Response Plan, and the appropriate sequence should be determined and communicated by the Emergency Response Plan administrator based on the systems that have been affected.
d. If required, the public and media outlets should be notified of the incident.

Return to Checklist

EXHIBIT 1: DATA CLASSIFICATION TEMPLATE

Example Data Classification Template

Data	Classification	Justification	Data Owner	Data User
Executive Business Material	Restricted Confidential	Intellectual Property		Executives & Assistants
Bank Accounts - Information	Confidential	SOX		Financial Reporting
Financial Reporting Data	Confidential/Public - phases	SOX		Financial Reporting
Building Information	Confidential	SOX		Financial Reporting
Legal Case Information	Sensitive	Intellectual Property		Legal
Leasing Information	Confidential / Restricted Confidential phases	Intellectual Property		Leasing
Security video	Sensitive	Intellectual Property		Security
Custom Application Code	Sensitive	Intellectual Property		Information Services
Audit Information	Restricted Confidential	Data from all areas		Audit Services
Tax Filings	Sensitive			Corporate Tax
HR	Sensitive	PII, Laws		HR
Benefits	Confidential	HIPAA / do not submit		HR

Definitive guide to data classification:

https://infosecpartners.com/wp-content/uploads/2017/02/The-Definitive-Guide-to-Data-Classification.pdf

6 EXHIBIT 2: CRITICAL ASSET INVENTORY PER FACILITY

Facility Name: _____

AssetID	Item	Description	Serial #	Service Date	Retirement Date	Original Value	Current Value	Custodian	Department

7 EXHIBIT 3: POLICY EXAMPLES

Policy Name	Description
Security Policy	A document designed for staff that should include the security program requirements and require signoff for employees.
Emergency Response Plan	Procedures to follow in the event of a Cybersecurity breach.
Password Policy	Outlines the specific password requirements for the organization.
Acceptable Use Policy	Defines how the internet and email should be used to promote a responsible culture around Cybersecurity.

- Guide to Industrial Control Systems (ICS) Security
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- Guide for Cybersecurity Event Recovery
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf
- 21 Steps to Improve Cyber Security of SCADA Networks
  https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf
- Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems
  https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf
- 10 ways to develop cybersecurity policies and best practices
  https://www.zdnet.com/article/10-ways-to-develop-cybersecurity-policies-and-best-practices/
- SANS Information Security Policy Templates
  https://www.sans.org/security-resources/policies

8 Exhibit 4: Water Waste Water Risk Assessment (To Be Delivered)

9 EXHIBIT 5: EMPLOYEE TRAINING AND AWARENESS

a. Implement a cybersecurity awareness program that includes:
    i. Social engineering
    ii. Sharing of personal information
    iii. Phishing
    1. Types of phishing attacks
    2. What can happen as a result of Phishing
    iv. Ransomware
    1. What to do in the event your system has been compromised by Ransomware
    v. Email Best Practices and what to watch for
    vi. Internet browsing acceptable use policy
    vii. Authentication (password policy, use of multi-factor authentication, and remote access where required).
b. Provide on-going cross training for critical systems and ICS staff that identifies current best practices and standards for ICS cybersecurity.
c. Provide basic network and radio communications training for ICS technicians.
d. Participate in water sector programs that facilitate cybersecurity knowledge transfer.
e. Identify appropriate certifications for internal and external staff. Include certification requirements in SLAs and contracts with external service providers.
f. Provide periodic security awareness training to employees that identifies risky behaviors and threats.
g. Promote information sharing within your organization.

10 EXHIBIT 6: SECURING NETWORK AND CLOUD

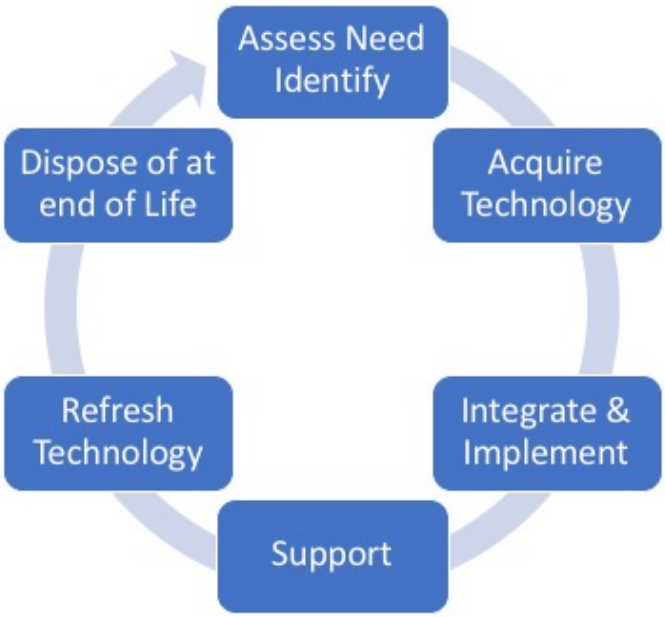
a. Network
    i. Network Separation
        1. Business systems such as email or other systems that require access to the internet should be managed on a separate physical network from the water/wastewater operation systems.
        2. A DMZ should be established for any traffic originating from outside of the internal network, although traffic of this origin should be eliminated where possible and ensure there is no connectivity to the Water/Wastewater systems network.
    ii. Network Hardware
        1. Have records of current hardware and software configurations.
        2. Maintain support contracts with critical software vendors, for example: endpoint protection (anti-virus, malware detection, log monitoring) and operating system patches in accordance with each vendor's recommended patch level if applicable
        3. It is important to maintain support contracts for software programs required to maintain the operation or protect/backup the systems.
            a. There could also be a delay in gaining access to critical software patches or system support if there is a lapse in support coverage.
            b. Software patches should be first tested on an offline system that doesn't have access to the Water/Wastewater Industrial Control System network.
            c. Once the patch is demonstrated to be safe, it can be scheduled on actual production systems.
    iii. Monitoring
        1. An NMS should be implemented to ensure alerts are sent to the network manager when a device is unavailable for a pre-determined period of time.
        2. System and Event Logs should be monitored for critical events that occur, and alerts sent to the network manager.
    iv. Cloud
        1. Interfacing with cloud environments
        2. IPSEC tunnels should be used between on premises networks and public cloud networks
        3. Firewalls should be used in cloud-based network for separation in the same manner recommended on internally hosted systems.
        4. Centralized authentication authority and multi-factor authentication should be used when accessing public cloud environments.
b. Server and Workstation Hardening:
    i. Disable services that are not required
        1. Use whitelisting software to only allow execution of required applications.
        2. Ensure system-based firewalls are not more permissive than they need to be – only allow what is absolutely necessary.
        3. Disable built-in, default accounts.
        4. Access Control should be employed and provide multi-factor authentication, pass phrases made up of 4 regular words, and unique passwords for different systems. Operational systems and Business systems should reside on two separate physical networks separated by firewall devices.
        5. Service Level Agreements (SLAs) should be included in vendor contracts to ensure they are providing the amount of internet bandwidth and round-trip speeds agreed

to in the contract, and that 3rd party personnel that work on utility systems are certified based on agreed upon industry standard certifications based on their job function.

c. Wireless and Wireless guest access secured by strong protocols, such as WPA2 with AES encryption.

11 Exhibit 7: Maintenance Life Cycle Process

Asset Lifecycle Management Process



12 EXHIBIT 8: EMERGENCY RESPONSE PLAN (ERP)

An emergency response plan (ERP) is important if a cybersecurity incident were to occur that requires notification outside of the primary business. The following is a guide for possible ERP action items:

1. Contact Law Enforcement-if required
2. Contact government authorities-if required
3. Notify customers
4. Record the data lost or exposed
5. Record measures taken to reduce future exposure
6. Technical and leadership work to limit damage
7. Containment
8. Reputation risk management
9. Request outside assistance if needed
10. Begin recovery
11. Eradicate malware
12. Hold lessons learned meeting
13. Discover knowledge gained during the incident
14. Document knowledge gained during the incident
15. Refine knowledge gained during the incident

13 EXHIBIT 9: CONTACT LIST

Contact Name	Organization Name	Phone	Email	Website
	Law Enforcement			
	IT Staff/Vendor			
	SCADA Staff/Vendor			
	DHS NCCIC	888-282-0870		
	Local Laboratory			
	State Primacy Agency			
	Local Emergency Management Agency			
	Local Health Department			
	IWARN Chair			
	State Emergency Management Agency			

14 Exhibit 10: After Action Report

Incident Name	[Insert the formal name of exercise, which should match the name in the document header]
Incident Dates	[Indicate the start and end dates of the incident]
Description	This incident …
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor)]

[Incident]

The strengths and areas for improvement for each core capability aligned to this objective are described in this section.

[Incident Description]

Strengths

The [full or partial] incident can be attributed to the following:

1: [Observation statement]

2: [Observation statement]

3: [Observation statement]

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: [Observation statement. This should clearly state the problem or gap; it should not include a recommendation or corrective action, as those will be documented in the Improvement Plan.]

Reference: [List any relevant plans, policies, procedures, regulations, or laws.]

Analysis: [Provide a root cause analysis or summary of why the full capability level was not achieved.]

Area for Improvement 2: [Observation statement]

Reference: [List any relevant plans, policies, procedures, regulations, or laws.]

Analysis: [Provide a root cause analysis or summary of why the full capability level was not achieved.]