ENERGY COMMITTEE STRATEGIC PLAN

Chair: Danielle McGrath
Co-Chair: Robert I. Richhart

October 2021
Indiana Executive Council on Cybersecurity

Energy Committee Plan

Table of Contents

Committee Members

Committee Members

Last Name	First Name	Organization	Organizational Title	Member Type (Chair/Co-chair/Full-time, As needed)
Aikman	J. Kurt	MISO Energy	Senior Security Advisor	Full Time
Berry	Scott	Indiana Municipal Power Agency	Compliance Manager	Full Time
Bowen	Brandon	Indiana Utility Regulatory Commission	Senior Utility Analyst	As Needed
Bowers	Scott	Hoosier Energy REC	Sr. VP Government and Community Relations	Full Time
Brown	Allen	Midwest Natural Gas	IT Director	Full Time
Cassady	John	Wabash Valley Power	Executive Vice President, Public Policy & Advocacy	Full Time
Chrislip	Chris	EICORP	Senior Cybersecurity Architect	As Needed
Dessuit	Frank	NIPSCO	Ops Technology and Security Manager	Full Time
Ellis	Greg	Indiana Chamber of Commerce	Vice President, Energy and Environmental Policy	Full Time
Garmon	Joe	Wabash Valley Power	Director of IT Policy and Cyber Security	Full Time
Willis	Corey	Indiana Electric Cooperatives (IEC)	VP, Information Services	Full Time
Hadley	Ryan	Indiana Utility Regulatory Commission	Executive Director of External Affairs	As Needed

Holmes	Evan	CenterPoint	Manager, Control Systems	Full Time
Krevda	Stefanie	Indiana Utility Regulatory Commission	Commissioner	As Needed
McGrath	Danielle	Indiana Energy Association	President	Chair
Richhart	Robert	Hoosier Energy REC	Chief Technology Officer	Co-Chair
Souza	Tony	Duke Energy	Director, Cybersecurity Architecture, IT/OT & TVM	Full Time
Swick	Steve	American Electric Power (AEP)/Indiana Michigan Power (I&M)	Chief Security and Privacy Officer	As Needed
Taylor	Curtis	Wabash Valley Power	Executive Vice President, Technology Services	Full Time
Wright	Carolyn	Indiana Municipal Power Agency	Vice President, Government Relations	Full Time
Miller	Scott	Citizens Energy Group	Manager of Security and Compliance	Full Time
Bailey	Gerry	Corvano LLC	President	As Needed
Day	David	MISO Energy	Consulting Information Security Analyst	Full Time

Introduction

Introduction

The world of cybersecurity is highly complex and cluttered with information, misinformation, and disinformation. As a consequence, it is important to approach it strategically and create simplicity.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

Executive Summary

Executive Summary

- **Research Conducted**
  - Assessed national regulations and cybersecurity guidelines
  - Assessed what Subsector Cybersecurity Coordinating Councils exist and their level of activity
  - Assessed the presence and value of sector-specific Information Sharing and Analysis Center (ISAC)
  - Assessed state-level guidelines
  - Reviewed National Association of Regulatory Utility Commissioners (NARUC) Cybersecurity Manual
  - Formulated needs for training by educational institutions to provide cybersecurity professionals
  - Determined level of interaction and need for interaction with other subsectors
  - Researched level of understanding of state priorities and response in a cyber emergency
  - Assessed what information is needed from other Committees/Work Groups on the Council

- **Research Findings**
  - The North American Electric Reliability Council (NERC) and Federal Energy Regulatory Commission (FERC) have set regulations on the electric utility industry. These are mandatory, and fines can be levied. The U.S. Transportation and Safety Administration (TSA) has Pipeline Security guidelines for natural gas utilities.
  - The electric utility industry, along with the nuclear industry, are the only critical infrastructure sectors which have mandatory, enforceable federal regulations in place for cybersecurity.
  - NARUC has resources for public utility commissions to gather and evaluate information from utilities about their cybersecurity risk management and preparedness.
  - On the national level, the Electric Subsector Coordinating Council and Oil & Natural Gas Subsector Coordinating Council are both quite active.
  - According to the National Conference for State Legislatures, the most commonly introduced bills seek to establish a state-level committee dedicated to studying cybersecurity and providing policymakers with recommendations.
  - Electric ISAC and Downstream Natural Gas ISAC are active.
  - Significant need for education and training exists.
  - Other subsectors, including for example Telecommunications and Financial, need to interact.

- **Committee Deliverable**
  - Critical Infrastructure Information (CII)
  - Training
  - Indiana Utility Regulatory Commission (IURC) Cybersecurity Forum
  - Resource Guide
  - Deliverable Workplace IT

- **Additional Notes**
  - None

- **References**
  - None

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. The electric and natural gas utility industry recognizes that the production, transmission, and distribution of electricity and natural gas is critical to the broader economy and well-being of Hoosiers. This industry is also heavily regulated, including cybersecurity. As a result, the industry has invested heavily to increase staffing, train employees, adopt the National Institute of Standards and Technology (NIST) framework and participate in tabletop exercises. An example of a training exercise is Grid-Ex. Grid-Ex is a biannual, nation-wide exercise which provides utilities a chance to "experience" a cyberattack. GridEx V in 2019 included more than 500 electric utilities, government and law enforcement agencies, and other organizations. GridEx VI is scheduled for November 16–17, 2021.
    b. At the national level, an Electric Subsector Coordinating Council (ESCC) and Oil & Natural Gas Subsector Coordinating Council were created to formalize communications between government and utilities. In addition, the Energy Information Sharing and Analysis Center (E-ISAC) is a sector-specific information sharing clearinghouse that includes downstream natural gas distribution companies operating in Indiana. The E-ISAC provides threat information and analysis. Separately, a Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC) is a leading threat information and analysis resource for natural gas utilities operating in Indiana.

2. **What (or who) are the most significant cyber vulnerabilities in your area? Are these components cybersecure?**
    a. Cyber vulnerabilities of components that are purchased and then installed in the energy network
    b. Communication between sectors (e.g., threats that are detected by another sector that others should be aware of)
    c. Potential disruptions of the telecommunications networks

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. There is continued need to enhance the educational capabilities in Indiana to train and educate individuals to work in cybersecurity.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Electric utilities are required to meet standards set by the North American Electric Reliability Council (NERC) and adopted by the Federal Energy Regulatory Commission (FERC). FERC regulations are binding and have the force of law. These standards have led to utilities adopting the NIST framework and implementing strong cybersecurity protocols, procedures and processes. The natural gas utilities work closely with the U.S. Transportation & Safety Administration (TSA). The TSA announced in July 2021 the issuance of a second Security Directive. This directive requires owners and operators of designated critical pipelines that transport hazardous liquids and natural gas to implement specific mitigation measures to protect against ransomware attacks and other known threats to information and operational technology systems. Critical Pipelines are also required to develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review. This is the second Security Directive that TSA has issued to the pipeline sector in 2021.

    The May 2021 Security Directive requires critical pipeline owners and operators to:
    1. report confirmed and potential cybersecurity incidents to CISA;
    2. designate a Cybersecurity Coordinator to be available 24 hours a day, seven days a week
    3. review current practices; and,
    4. identify any gaps and related remediation measures to address cyber-related risks and report the results to TSA and CISA within 30 days.

5. **What case studies and/or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. Both electric and natural gas facilities are a part of a national network. As such, issues are addressed recognizing that a cyberattack may impact large geographic areas and would not be limited to a single state. Electric utilities have conducted biennial exercises to test responses to such a large-scale outage. This training exercise is known as GridEx.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc.**
    a. Attached are several documents which provide more details on these issues. (See Supporting Documentation)

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. Since energy companies are required to meet the same regulations or guidelines, training in the energy industry is similar across the country. , Energy utilities engage in national and localized exercises.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Year One
        i. Energy providers of all sizes have access to cybersecurity resources for the purpose of bolstering their own internal cybersecurity plans.
        ii. Energy providers have identified unique workforce challenges for the industry associated the pandemic and identified best practices.
    b. Year Three
        i. Utilities have, if needed, modified and/or strengthened their cybersecurity plans.
        ii. Energy providers continue to understand, assess and implement protocols for dealing with the integration and security associated with new technology.
        iii. The energy providers and the IURC have established communication channels for sharing cybersecurity information.
        iv. Contact lists are maintained and updated as needed.
    c. Year Five
        1. Ongoing evolution of the way we work together in Indiana has revised and changed as we respond to the ever-changing risk environment.
        2. Utilities have an ever-increasing number of graduates from Indiana educational institutions who work on cybersecurity issues.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. Indiana's educational institutions should be more intentional about training students for cybersecurity roles. Educational institutions need to increase awareness of the importance of these roles and alert students to the types of jobs available in the field.

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. Total Workforce
        - More than 12,000 direct employees.
    b. Cybersecurity-related workforce
        - More than 45 employees. However, this number is not reflective of the total number of employees focused on cybersecurity in the utility industry which serves Indiana customers. Several companies who serve significant numbers of Hoosiers have consolidated their cybersecurity efforts into enterprise-wide departments. Since the utility industry operations cross state boundaries, this allows companies to consider cyber risks and address those risks across a much larger footprint. Considering all of these employees, would show employment of several hundred individuals.
    c. Unmet cybersecurity-related workforce
        - While not a comprehensive assessment, each cybersecurity operation in the utility space would benefit from an increase in trained cybersecurity professionals.

11. What do we need to do to attract cyber companies to Indiana?

a. Vendors who work to address the issues raised in item 2a) and 2c) above in the Energy Committee Strategic Plan are areas for new companies to focus. Encouraging a robust business climate where new companies working to meet the needs of Indiana businesses can prosper is important.

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

a. Utilities operating in Indiana have established emergency operations centers for their companies. Individuals staffing these centers will be able to assess the nature of an incident and develop appropriate responses. These centers are also capable of communicating with other emergency operations centers. Communication protocols also include integrating the information from the Electric Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council.

13. What best practices should be used across the sectors in Indiana?

a. Best practices will be better assessed and implemented once more information on the current cybersecurity in other sectors is known. , The electric and natural gas industries have benefited from participation in Coordinating Councils and the sector-specific ISACs. Broadening the flow of information from one sector to another would facilitate implementation.

Deliverable: Critical Infrastructure Information (CII)

Deliverable: Critical Infrastructure Information (CII)

General Information

1. **What is the deliverable?**
    a. Review potential policy changes to protect critical infrastructure information while maintaining public access and freedom of information.

2. **What is the status of this deliverable?**
   ☒ Completed ☐ In-progress 25% ☐ In-progress 50%. ☐ In-progress 75%. ☐ Not Started

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. In 2018, the Energy Committee determined that additional laws or policies were not needed in Indiana. We are conducting a new review to determine whether policy action is warranted now and will be examining different resources and engaging the broader energy industry.

6. **What metric or measurement will be used to define success?**
    a. The electric and natural gas companies need a stable policy environment which provides flexibility to adapt to the ever-changing attacks. In particular, a consistent set of policies is important without conflicting provisions or policies which place activity above assuring security are needed. Finally, this industry is strongly

interconnected across state lines. Hence, existing regulation is often appropriate to avoid conflicting requirements. Success will be measured by assuring consistent, flexible policies most likely implemented at the federal level.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Customers, energy companies, law enforcement, disaster response personnel, media, and many others would benefit.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. At this point, there is not a notable or problematic overlap.

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 that the electric and natural gas operating environment is unique in having already implemented mandatory regulations and/or guidelines which impact companies across the nation and in Indiana. We would anticipate that other members of the IECC may determine that policy level changes are needed. There may be lessons to be learned by others from reviewing the long-standing regulations and guidelines established by the NERC or the TSA. We will engage with other committees/working groups and attempt to accomplish their goals without impeding this industry's ability to implement strong cybersecurity programs.

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. Given almost all Hoosiers use of electricity and natural gas, it becomes important to interface with virtually all other sectors. However, among the most critical will be the US Department of Energy (DOE), Department of Homeland Security (DHS), TSA and FERC; the Indiana Department of Homeland Security (IDHS) and Utility Regulatory Commission (IURC); the NERC as well as Congress and the Indiana General Assembly. Similarly, law enforcement will need to be involved, whether that is the Federal Bureau of Investigation (FBI) or the Indiana State Police (ISP); lest they be overlooked, all aspects of the energy industry, including those represented on the IECC Energy Committee, will need to be involved.

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Danielle McGrath at the Indiana Energy Association. It is her responsibility to share the information with the Energy Committee and to provide feedback to others.

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

a. None.

Implementation Plan

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

☒ One-time deliverable

☐ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Critical Infrastructure Information (CII) in the energy industry is defined by federal entities.	FERC and the TSA	100%	9/30/21	
Engage statewide energy industry stakeholders to determine whether state-level policy changes are warranted.	Indiana Energy Association Indiana Municipal Power Agency Indiana Electric Cooperatives Indiana Chamber Indiana Utility Regulatory Commission	75%	12/2021	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
None	None				

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
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Consistent definition of CII occurs in the highly interconnected network of electric and natural gas facilities which reach across state lines.

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

a. Efficient communications as well as protecting key assets and information from "bad actors" will reduce cyber risk. These costs are already a part of operating our utilities. We do anticipate that costs will arise as the issues mature and become more challenging.

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

a. This deliverable is already completed.

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

a. CII definitions are in place and are being used. These have been in place and their use will continue.

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

☒No ☐ Yes

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

☒No ☐ Yes

Other Implementation Factors

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

a. The cost of using the CII definitions is already a part of the energy industry cost structure.

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

☒No ☐ Yes

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

a. These supports are already in place within the energy utilities operating in Indiana.

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

a. These definitions of CII have already been implemented within the utility sectors. An example of the definitions appears in the Energy Committee Strategic Plan. These definitions were taken from the FERC website and can be reached at the following hyperlink. https://www.ferc.gov/legal//maj-ord-reg/land-docs/ceii-rule.asp

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. Use by others may be possible; however, utilities are highly technical with unique operational characteristics, and we suspect that not all definitions will translate well to other sectors.

Communications

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

a. These are existing at the moment and have been implemented. Information has been shared by the industry. However, to the extent that others are not aware of this, they can contact the Energy Committee.

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

☐No ☒ Yes

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

a. We do not see this item as key for either public relations or marketing consideration.

Evaluation Methodology

Objective 1: IECC Energy Committee will provide a review of the July 2018 definitions by October 2021.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Objective 2: IECC Energy Committee will review potential state policy changes to protect critical infrastructure information while maintaining public access and freedom of information by December 2021.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Deliverable: Training

Deliverable: Training

General Information

1. **What is the deliverable?**
    a. Training
        i. Objective 1: Develop a survey to determine whether there are new training needs specific to the energy industry following the pandemic.
        ii. Objective 2: Identify and recommend opportunities at the state, vocational, or higher education level.

2. **What is the status of this deliverable?**
☐ Completed ☒ In-progress 25% ☐ In-progress 50%. ☐ In-progress 75% ☐ Not Started

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Our deliverable is to support others with a clear understanding of what the energy industry needs in training and education to support and enhance energy company cybersecurity, including identifying skill gaps and recommending opportunities to address them.

6. **What metric or measurement will be used to define success?**
    a. Identified training resources for identified training needs.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. All energy sector entities of various sizes.

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

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Workforce Development Committee. Feedback from energy sector survey participants.

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. DHS, CISA, educational institutions and etc.

12. **Who should be the main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Danielle McGrath at the Indiana Energy Association. It is her responsibility to share the information with the Energy Committee and to provide feedback to others.

13. **What are the expected challenges to completing this deliverable?**
    a. This will be best defined by the Committees and Working Groups who are directly developing the needed training.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Coordinate with Workforce Development Committee.	Energy Committee	10%	08/2021	
Develop survey content.	Energy Committee	0%	08/2021	
Distribute survey.	Energy Committee	0%	09/2021	
Analyze results	Energy Committee	0%	10/2021	
Research training opportunities to meet gaps	Energy Committee	0%	11/2021	
Develop recommendations.	Energy Committee	0%	12/2021	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
Minimal	Minimal	Project Management	Existing payroll of Energy Committee Members	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
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Address training gaps to promote reliability and resiliency.

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

a. Better skilled employees reduce the risk of mistakes and oversights as we strive to protect utility operating systems or to recover should an incident occur. The Workforce Development Committee is likely a better source to assess the cost of developing the needed programs.

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

a. Insufficiently trained employees.

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

a. Success is having Hoosiers who possess the skills the energy industry needs.

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

☐No ☒ Yes

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

☐No ☒ Yes

Other Implementation Factors

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

a. None

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

☒No ☐ Yes

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

a. Annual review

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

a. In responses to the questions asked in Phase 1, we have asked for support from the Workforce Development Committee.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. We believe that all sectors will benefit from enhanced training in the skills needed for cybersecurity.

Communications

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

a. All committees and working groups could benefit from this deliverable.

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

☐No ☒ Yes

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

a. It would be an opportunity to highlight Indiana's educational system's ability to train individuals in an evolving technical workplace.

Evaluation Methodology

Objective 1: Develop a survey to determine whether there are new training needs specific to the energy industry following the pandemic by October 2021.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

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

Objective 2: Identify and recommend opportunities at the state, vocational, or higher education level December 2021.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

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

Deliverable: IURC Cybersecurity Forum

Deliverable: IURC Cybersecurity Forum

General Information

1. **What is the deliverable?**
   a. Host a forum for small natural gas utilities to share information and best practices on cybersecurity.

2. **What is the status of this deliverable?**
   ☐ Completed ☒ In-progress 25% ☐ In-progress 50%. ☐ In-progress 75%. ☐ Not Started

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable**?
   a. The purpose of the goal is to assess small gas operators' (less than 35,000 customers) cybersecurity preparedness and provide tools, resources, and information to guide them towards a greater understanding of their cybersecurity needs.

6. **What metric or measurement will be used to define success?**
   a. Completion rate of survey(s) and attendance at the in-person forum.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. IURC-regulated public gas utilities that serve generally less than 35,000 customers.

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. None.

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. The Indiana Department of Homeland Security (IDHS), U.S. Department of Homeland Security (U.S. DHS), the Indiana Energy Association (IEA), the American Gas Association (AGA), the U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA), and the invited utilities, including:
       - Boonville Natural Gas Corp.
       - Community Natural Gas Go., Inc.
       - Fountaintown Gas Co., Inc.
       - Indiana Natural Gas Corp.
       - Midwest Natural Gas Corp.
       - Ohio Valley Gas Corp.
       - South Eastern Indiana Natural Gas Co., Inc.
       - Sycamore Gas Co.
       - Switzerland County Natural Gas Co.

12. **Who should be main lead of this deliverable?**
    a. Stefanie Krevda, IURC/Ryan Hadley, IURC

13. **What are the expected challenges to completing this deliverable?**
    a. Securing expert speakers for the event; setting an appropriate date for the forum that all parties can attend.

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability? Within the Commission we plan to regularly engage with our regulated utilities regarding cybersecurity matters; however, for the IECC sub-committee it will not.

☒ One-time deliverable

☐ Ongoing/sustained effort

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Develop cybersecurity survey and send to small gas operators	Stefanie Krevda/Ryan Hadley	100%	6/4/2021	Confidential survey sent and responses received by most gas operators on June 4, 2021.
Evaluate responses and develop list of topics for forum	Stefanie Krevda/Ryan Hadley	25%	8/1/2021	
Set date and time for cyber forum	Stefanie Krevda/Ryan Hadley	0%	9/1/2021	
Secure speakers for cyber forum	Stefanie Krevda/Ryan Hadley	0%	10/31/2021	
Host cyber forum	IURC	0%	Qtr. 1 2022	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

Estimated Initial FTE	**Estimated Continued FTE**	**Skillset/Role**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
None	None		This type of work is already captured in the IURC and energy provider budgets.		

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

a. No Response

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. The greatest benefit of the deliverable is two-fold: (1) education for regulators and small gas operators; and (2) provide resources for small gas operators to develop more mature cybersecurity protocols, as they determine applicable for their organizations.

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

a. The deliverable will reduce cybersecurity risk by educating small gas operators on the importance of evaluating and incorporating appropriate cybersecurity measures to mitigate risks and impacts to their systems. The estimated costs associated with risk reduction can range depending on the implemented steps, but likely in the thousands of dollars.

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

a. Cybersecurity risks can impose a great deal of costs if left vulnerable to attack. Small gas operators could lose their IT systems to ransomware, resulting in costs ranging in the thousands of dollars. However, if a cyberattack cripples their operational infrastructure, that could cost millions to replace, depending on the extent of the damages.

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

a. The baseline for evaluation is the survey results received from the small gas operators. The metric for success would be attendance at the in-person forum to hear from cybersecurity experts and increased cyber hygiene. Future cyber surveys will reveal an improvement their preparedness.

21. Are there comparable jurisdictions (e.g., other states) that have similar projects using the same metrics?

☒No ☐ Yes

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

☒No ☐ Yes

Other Implementation Factors

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

a. Generally speaking, any staff turnover at the IURC that impacts its ad-hoc cybersecurity working group may impact the requisite resources required to achieve the deliverable.

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

☒No ☐ Yes

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

a. 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?

☐No ☒ Yes

a. Water

Communications

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

a. The Energy Committee of the IECC.

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

☐No ☒ Yes

Note: The cybersecurity surveys and results should not be included as they are confidential and exempt from disclosure, but a summary and posting of the agenda of the Executive Session can be made available.

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

a. We do not necessarily see this item as a key for either public relations or marketing consideration.

Evaluation Methodology

Objective 1: Indiana Utility Regulatory Commission (IURC) will host a cybersecurity forum for small natural gas utilities to share industry information and best practices by December 2021.

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Deliverable: Resource Guide

Deliverable: Resource Guide

General Information

1. **What is the deliverable?**
    a. The deliverable is to develop a resource guide for all Indiana energy companies that helps identify emerging technology and supply chain issues and provides guidance and information to establish uniform and effective methods for cybersecurity protection across the entire energy sector.

2. **What is the status of this deliverable?**
☐ Completed ☒ In-progress 25% ☐ In-progress 50%. ☐ In-progress 75%. ☐ Not Started

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The development and sharing of a resource guide that informs all Energy Sector entities of uniform and effective policies, methods, and processes to protect their assets from malicious cybersecurity intrusions and potential system compromise.

6. **What metric or measurement will be used to define success?**
    a. A published resource guide for use by all energy sector entities.

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

   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. All energy sector entities

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

Additional Questions

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

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. Key resources may include DHS CISA, EISAC, Indiana National Guard and possibly others.

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Danielle McGrath at the Indiana Energy Association. It is her responsibility to share the information with the Energy Committee and to provide feedback to others.

13. **What are the expected challenges to completing this deliverable?**
    a. The everchanging threat landscape and acquiring resources. Developing comprehensive list of current resources for inclusion in resource guide.

Implementation Plan

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

    ☐ One-time deliverable

    ☒ Ongoing/sustained effort

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Gather information available across the sector and from other resources for development of the resource guide	Energy Committee	25%	3/1/2022	
Develop Resource Guide	Energy Committee	0%	Qtr. 3 2022	
Disseminate Resource Guide	Energy Committee	0%	Qtr. 4 2022	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

Estimated Initial FTE	**Estimated Continued FTE**	**Skillset/Role**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
None					

16. What other resources are required to complete this deliverable?

Resource	**Justification/Need for Resource**	**Estimated Initial Cost**	**Estimated Continued Cost, if Applicable**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Sharing of knowledge, best practices, and resources regarding cybersecurity protection

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

a. Yes, the availability of this resource will help to reduce the potential cybersecurity risk by sharing information to help all energy sector entities to improve their cybersecurity protection processes in a uniform and effective manner.

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

a. Lack of awareness around industry best practices and resources

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

a. Improved awareness for all energy sector entities of best practices and processes to adequately protect against malicious cybersecurity incidents.

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

☒No ☐ Yes

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

☒No ☐ Yes

Other Implementation Factors

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

a. None

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

☒No ☐ Yes

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

a. Annual review and refresh

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

a. No Response

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. Any critical sector

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

a. All energy utilities across state

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

☐No ☒ Yes

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

a. None

Evaluation Methodology

Objective 1: The IECC Energy Committee will define emerging technology and supply chain issues related to the grid Qtr. 3 2022.

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Objective 2: The IECC Energy Committee will determine whether best practices and information are widely available Qtr. 3 2022.

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Objective 3: The IECC Energy Committee will develop an industry specific resource guide Qtr. 4 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Deliverable: Workplace IT

Deliverable: Workplace IT

General Information

1. **What is the deliverable?**
    a. To develop a survey to capture cybersecurity challenges that the energy sector has faced as a result of workforces moving to work-from-home models. Identify best practices within the survey respondents and/or industry standards and share those results with the energy sector.

2. **What is the status of this deliverable?**
☐ Completed ☐ In-progress 25% ☐ In-progress 50%. ☐ In-progress 75%. ☒ Not Started

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Increased awareness within the energy sector of the challenges introduced by a remote workforce and awareness of best practices to address those challenges.

6. **What metric or measurement will be used to define success?**
    a. The dissemination of survey results and industry best practices.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Energy sector and partners in similar industries

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

Additional Questions

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

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 Energy Association, Indiana Electric Cooperatives, Indiana Municipal Power Agency

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Danielle McGrath at the Indiana Energy Association. It is her responsibility to share the information with the Energy Committee and to provide feedback to others.

13. **What are the expected challenges to completing this deliverable?**
    a. Asking the correct questions in the survey and targeting the correct audience

Implementation Plan

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

☒ One-time deliverable

☐ Ongoing/sustained effort

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Develop survey content	Energy Committee	0%	08/2021	
Distribute survey	Energy Committee	0%	09/2021	
Analyze results	Energy Committee	0%	10/2021	
Identify trends/best practices in survey responses	Energy Committee	0%	11/2021	
Identify industry best practices (NIST, CERT) to reference for best practices	Energy Committee		12/2021	
Develop and distribute recommendations.	Energy Committee	0%	2/2022	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

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

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

a. No Response

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

Benefits and Risks

17. What is the greatest benefit of this deliverable?

- **a.** Providing energy sector members with best practices and industry resources to manage a remote workforce.

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

- **a.** By establishing better processes and controls to manage the risk of a remote workforce. Costs of implementing such measures will be unique to each organization.

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

- **a.** Increased cyber risks to the energy sector due to poorly controlled and managed remote workforce.

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

- **a.** Success is defined by providing energy sector member with the tools and resources to better mitigate cyber risks.

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

☒No ☐ Yes

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

☒No ☐ Yes

Other Implementation Factors

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

- **a.** None

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

☒No ☐ Yes

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

a. Not ongoing

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

- **a.** Workforce Development

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. Water/Wastewater Sector and other sectors with industrial control systems

Communications

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

a. Energy Sector and Workforce Development

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

☒No ☐ Yes

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

a. Coordinating with industry groups to distribute the survey

Evaluation Methodology

Objective 1: The IECC Energy Committee will develop a survey to identify challenges in the workplace for the energy sector in Qtr. 4 2021.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Objective 2: The IECC Energy Committee will identify issues stemming from the work-from-home environment in Qtr. 4 2021.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Objective 3: The IECC Energy Committee will share best practices and coordinate with other sectors as needed in Qtr. 1 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Supporting Documentation

Supporting Documentation

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

- American Public Power Association (APPA) – Cybersecurity and the Electric Sector – July 2021
- Electricity Subsector Coordinating Council (ESCC) - Cyber Mutual Assistance Program Brochure - January 2021
- Federal Energy Regulatory Commission (FERC) Critical Energy/Electric Infrastructure Information (CEII) Regulations - 2020 - 2020

American Public Power Association (APPA) – *Cybersecurity and the Electric Sector*

ISSUE BRIEF June 2021

Grid Security

Summary

A reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans. Public power utilities, together with the entire electric utility industry, take very seriously their responsibility to maintain a secure and reliable electric grid. It is the only critical infrastructure sector that has mandatory and enforceable federal regulatory standards in place for cyber and physical security (collectively known as grid security). Cyber-attacks, relatively new compared to long-known physical threats, have rapidly evolved and could have operational consequences. The American Public Power Association (APPA) believes that the industry and its federal government partners have made great strides in addressing cybersecurity threats, vulnerabilities, and potential emergencies. Given the persistence and sophistication of threats, APPA knows that utilities cannot prevent all attacks at all times. For both cyber and physical threats, electric utilities employ risk management programs to prioritize facilities and equipment, develop contingency plans, and employ defense-in-depth techniques to keep the lights on.

Key Pillars of Grid Security

Mandatory and Enforceable Standards

The electric utility sector is the only critical infrastructure sector (besides the nuclear power sector, a part of the overall sector) that has a mandatory and enforceable federal regulatory regime in place for cybersecurity. Congress approved the standards regime for the bulk power system in the Energy Policy Act of 2005 (EPAct05) (section 215 of the Federal Power Act (FPA)). Under section 215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities, and government representatives, regularly drafts reliability, physical security, and cybersecurity standards that apply across the North American grid, including Canada.[1] Participation by industry experts and compliance personnel in the NERC critical infrastructure protection (CIP) standards development process ensures that the standards are technically sound, fair, and balanced. The Federal Energy Regulatory Commission (FERC) has the power to then approve or remand those standards as they apply in the United States. To ensure compliance, under FERC's oversight, NERC and its regional entities conduct rigorous audits and can levy substantial fines for non-compliance. Additionally, FERC can instruct NERC to develop new or revised reliability standards with a very short turn-around time.

CIP standards establish an important baseline of security—but they are a floor, not a ceiling—and grid security is and should be much more than a compliance exercise.

Information Sharing

Industry has long recognized that increased information sharing and appropriately tailored liability protection would further enhance the industry's ability to guard against cyber-attacks. As such, APPA strongly supported passage of the Cybersecurity Act of 2015, which was incorporated as Division N of

[1] NERC standards cover the Bulk Electric System (BES).

P.L. 114-133, the Consolidated Appropriations Act, 2016. The act provides policies and procedures for sharing cybersecurity threat information between the federal government and private entities (which includes electric utilities), as well as sharing between private entities while providing limited liability protection for these activities if conducted in accordance with the act.

In addition to the Cybersecurity Act of 2015, APPA also strongly supported section 61003 of P.L. 114-94 (the Fixing America's Surface Transportation Act or "FAST Act"), which gave the Secretary of Energy broader authority to address grid security emergencies under the FPA. It also clarified the ability of FERC and other federal agencies to protect sensitive critical electric infrastructure information (CEII) from public disclosure under the Freedom of Information Act (FOIA) and other sunshine laws. Under the FAST Act, FERC-designated CEII is exempted from disclosure for a period of up to five years with a process to lift the designation or challenge it in court. In addition, it established sanctions for the unauthorized disclosure of shared information. It is critical to operational security that the industry is confident that sensitive information about critical infrastructure that might provoke new threats or endanger the integrity of the electric power grid not be publicized. CEII information in the public sphere creates a grave vulnerability to the electric power grid, by significantly reducing the surveillance effort required by dedicated domestic and foreign adversaries. APPA has supported legislation and actions by DOE and FERC that would further clarify and enhance the ability of the federal government and other stakeholders to maintain the confidentiality of CEII to minimize the risk that such information could be used by malicious actors to target grid infrastructure.

APPA strongly encourages its members to share physical security and cybersecurity related threats that they face to information sharing entities, such as the Electricity Information Sharing and Analysis Center (E-ISAC), as well as the Multi-State Information Sharing and Analysis Center. These information sharing organizations are critical to ensure that the broader public power community and the entire electric power industry have awareness of the tactics, techniques, and procedures used by the adversaries targeting the electric grid.

Public-Private Partnerships

The electric power industry works closely with the federal government, including NERC, FERC, DOE, and the Department of Homeland Security (DHS), on matters of critical infrastructure protection. One important venue for this collaboration is the Electric Subsector Coordinating Council (ESCC). The ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. APPA and public power utilities play a leadership role on the ESCC, which includes utility CEOs and trade association leaders representing all segments of the industry. Their counterparts include senior administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

APPA works directly with DOE on a number of fronts. Most recently, in September 2020, DOE's Office of Cybersecurity, Energy Security and Emergency Response (CESER) awarded APPA a grant of $6 million over a three-year period to develop and deploy cyber and cyber-physical solutions for public power utilities. The program's goal is to provide utilities with emerging innovations at the hardware, firmware, and/or software levels to protect key operation technology (OT) components that enable the safe control of the physical systems that deliver electric power. This effort builds on the accomplishments of another three-year grant CESER awarded to APPA in 2016, with which APPA assessed and helped to strengthen the cybersecurity posture of small- and medium-sized public power utilities. This grant enabled the development of a cybersecurity scorecard for public power utilities to assess their cyber readiness, the production of a cybersecurity roadmap, an incident response playbook, and other guidance documents to help utilities develop a culture of cybersecurity within their organization.

Legislation based on the success of the 2016 grant program has been introduced over the past three Congresses. Most recently Representatives Jerry McNerney (D-CA) and Bob Latta (R-OH) introduced H.R. 2931,the Enhancing Grid Security through Public-Private Partnerships Act, to permanently fund

public-private partnerships to promote and advance the physical and cybersecurity of electric utilities. The House Energy & Commerce Committee approved H.R. 2931 unanimously in June. APPA strongly supports the bill. There is not currently a standalone Senate companion, but a similar provision is included in a draft infrastructure bill by Senate Energy & Natural Resources Committee Chairman Joe Manchin (D-WV).

"Defense-in-Depth" and Sector-Wide Preparation Exercises

The goal of every utility and the entire industry is to manage risk prudently. Still, there are tens of thousands of diverse facilities throughout the U.S. and Canada that cannot be protected 100 percent of the time from all threats, requiring utilities to prioritize facilities that, if damaged, would have the most severe impacts on their ability to keep the lights on. As such, the electric power industry employs threat mitigation known as "defense-in-depth" that focuses on preparation, prevention, response, and recovery to "all hazard" threats to electric grid operations.

Electric utilities plan and regularly exercise for a variety of emergency situations that could impact their ability to provide electricity. One such exercise, GridEx V, took place in November 2019 and involved over 500 organizations and 7,000 participants from industry, government agencies, and partners in Canada and Mexico. APPA was significantly involved in the planning for GridEx V to further allow distribution utilities to get value from the distributed play portion of the exercise. One hundred public power organizations participated in the GridEx V distributed play, up from 53 that did so at GridEx IV in 2017. Managed by NERC and the E-ISAC, GridExV also included an executive tabletop exercise where 108 electric sector executives and senior U.S. government officials worked through incident response protocols to address widespread outages. GridEx events are conducted every two years; GridEx VI is scheduled for November 2021.

The three primary segments of the electric utility industry—public power, investor-owned, and rural electric cooperatives—have long had in place mutual aid response networks to share employees and resources to restore power after natural disasters and other emergencies. The ESCC used the concept of traditional mutual assistance networks to develop the Cyber Mutual Assistance program that can help electric and natural gas companies, public power utilities, and/or rural electric cooperatives restore critical computer systems following significant cyber incidents. The program now includes more than 170 entities across all segments of the industry, serving more than 80 percent of all U.S. electricity customers.

Finally, electric utilities regularly share transformers and other equipment through long existing bilateral and multilateral sharing arrangements and agreements. The industry is expanding equipment sharing programs—like the Spare Transformer Equipment Program (STEP), SpareConnect, and Grid Assurance—to improve grid resiliency.

Administrative Action

Supply Chain Security Executive Actions

On May 1, 2020, President Trump signed an Executive Order 13920 (EO or order), *Securing the United States Bulk Power System,* deeming "the unrestricted foreign supply of bulk-power system electric equipment" as an "unusual and extraordinary threat to national security." The order broadly prohibited any person subject to federal jurisdiction from acquiring, importing, transferring, or installing bulk-power system electric equipment designed, developed, manufactured, or supplied by foreign adversaries when those transactions pose an undue or unacceptable risk to the grid or national security. DOE was tasked with leading a broad inter-agency effort to further define and implement the order's requirements within 150 days. As part of the implementation of the EO, on December 17, 2020, DOE released a prohibition order aimed at reducing the risks that entities associated with China pose to the nation's BPS. The order, which took effect January 16, 2021, prohibited utilities that supply critical defense facilities from procuring from China specific BPS equipment that poses an undue risk to the BPS, the security or resilience

of critical infrastructure, the economy, national security, or safety and security of Americans. The order only applied to utilities that have been designated as defense critical electric infrastructure (DCEI); a small number of public power utilities have been notified that they have been designated as DCEI.

On his first day in office, President Joe Biden signed an Executive Order, *Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis,* that included a provision suspending EO 13920 for 90 days and directing DOE and the Office of Management and Budget to "jointly consider whether to recommend that a replacement order be issued." On April 20, DOE announced that it was revoking the December 17, 2020, prohibition order on securing critical defense facilities [EO 13920 itself was briefly reinstated following the 90-day suspension, but the emergency declaration of the EO expired on May 1]. In conjunction with the announcement that it was revoking the prohibition order, DOE announced a new request for information (RFI), "Ensuring the Continued Security of the United States Critical Electric Infrastructure," seeking input from stakeholders to inform future recommendations for supply chain security in U.S. energy systems. APPA submitted comments in response to the RFI on June 7, asking DOE to focus on four foundational principles as it considers further action on energy sector supply chain security: (1) new measures must be risked-based; (2) directives should be clear, prospective, and scalable; (3) directives must be cost-conscious; and (4) DOE should focus on vendor risks.

NSC "100 Day Industrial Control Systems Cybersecurity Sprint"

On April 20, the Biden administration announced that it was launching a new initiative to enhance the cybersecurity of electric utilities' industrial control systems (ICS). This 100 day "sprint" is a coordinated effort between the National Security Council (NSC), DOE, and the ESCC to encourage and support utilities' visibility and situational awareness into their ICS and OT networks. APPA, as the primary public power point of contact for the initiative, is working with public power utilities to facilitate their participation in this voluntary pilot program. This effort has appropriately raised the issue of ICS security to a higher priority in the federal government. APPA views this sprint as the start of a long journey of collaboration between public power and the federal government, which includes the work being done through the CESER grant to APPA.

APPA Position

The regulations and standards ("NERC-FERC") process set up in EPAct05 provide a solid foundation for strengthening the industry's security posture. These mandatory standards evolve with input from subject-matter experts from across industry and government. However, the industry recognizes that it cannot protect all assets from all threats all the time, and instead must manage risk. APPA believes that close coordination among industry and government partners at all levels is imperative to deterring attacks and preparing for emergency situations.

APPA Contact

Amy Thomas, Senior Government Relations Director, 202-467-2934 / athomas@publicpower.org

Jack Cashin, Director, Policy Analysis & Reliability Standards, 202-467-2979 / jcashin@publicpower.org

Nathan Mitchell, Senior Director, Operations Programs, 202-467-2925 / nmitchell@publicpower.org

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. We represent public power before the federal government to protect the interests of the more than 49 million people that public power utilities serve, and the 93,000 people they employ. Our association advocates and advises on electricity policy, technology, trends, training, and operations. Our members strengthen their communities by providing superior service, engaging citizens, and instilling pride in community-owned power.

Electricity Subsector Coordinating Council *(ESCC) - Cyber Mutual Assistance Program Brochure*

The ESCC's Cyber Mutual Assistance Program

The Electric Power and Natural Gas Industries Share Expertise to Counter Cyber Attacks

CMA

Cyber Mutual Assistance

Cyber Defense: Building on the Industry's Culture of Mutual Aid

The North American energy grid is a complex interconnected network of generation, transmission, and distribution systems operated by thousands of organizations. Protecting the energy grid and ensuring a reliable and affordable supply of energy are the top priorities of the electric power and natural gas industries. Creating a "defense-in-depth" approach requires partnerships and coordination with the government and other critical infrastructure sectors. To coordinate security strategies with the federal government and other stakeholders, the electric power industry has created a CEO-led partnership called the Electricity Subsector Coordinating Council (ESCC).

For decades, the electric power and natural gas industries have operated voluntary mutual assistance programs that work collaboratively to restore service following storms, earthquakes, wildfires, and other natural disasters. These mutual assistance programs provide a formal, yet flexible, process for companies to request assistance from one another.

Building on the industries' culture of mutual assistance, and informed by lessons learned from major destructive cyber incidents overseas as well as by exercises held in North America, the ESCC directed the formation of the Cyber Mutual Assistance (CMA) Program. The Program is a natural extension of the electric power and natural gas industries' longstanding approach of sharing critical personnel and equipment when responding to emergencies. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power and natural gas industries are enhancing our nation's ability to defend and protect against threats and to meet customers' expectations.

Delivering and Coordinating Cyber Mutual Assistance: How It Works

- The CMA Program is composed of industry cyber experts who are able to provide voluntary assistance to each other in advance of, or in the event of, a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency.
- Participation in the CMA Program is open to all entities that provide or materially support the provision of electricity or natural gas service.
- Participation in the CMA Program, as well as any decision to respond to requests for assistance made under the CMA Program, is voluntary.
- To participate in the CMA Program, entities must execute a mutual non-disclosure agreement so that all participants are assured that confidential information they may share will be protected.
- Participating entities also must designate an individual with appropriate cyber skills and experience, and the necessary authority, to represent the entity in the CMA Program (the CMA Coordinator).
- Cyber mutual assistance under the CMA Program is intended to be advisory and short-term. It may include services, personnel, and/or equipment.
- There is no cost to participate in the CMA Program other than the reimbursement of the costs and expenses of an entity providing emergency cyber assistance.

Frequently Asked Questions About Cyber Mutual Assistance

What is the Cyber Mutual Assistance Program?

The Cyber Mutual Assistance (CMA) Program is an industry framework developed at the direction of the ESCC to provide emergency cyber assistance within the electric power and natural gas industries. The CMA Program is composed of industry cyber experts who can provide voluntary assistance to other participating entities in advance of, or in the event of, a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency. As the CMA Program develops, additional initiatives will be considered and implemented based on the needs and input of the entities participating in the CMA Program.

How can I participate in the CMA Program?

To participate in the CMA Program, each participating entity must (1) sign a mutual non-disclosure agreement, and (2) designate a CMA Coordinator.

What does a CMA Coordinator do?

A CMA Coordinator is a participating entity's primary point of contact for all matters related to the CMA Program. He or she is responsible for assessing relevant cyber resources, considering and responding to another participating entity's request for assistance, and making any requests for emergency assistance on behalf of the entity he or she represents.

What are the qualifications for a CMA Coordinator?

A CMA Coordinator must be an individual with sufficient authority to act on behalf of the participating entity he or she represents. In addition, a CMA Coordinator must possess or manage sufficient cybersecurity, operating technology, and information technology skills and experience to be able to request, or respond to a request for, a broad range of emergency cyber needs in the context of a potentially complex and evolving cyber emergency.

How does the Program work?

In the event of a cyber emergency, any participating entity may make a direct request for assistance through its CMA Coordinator to any other CMA Coordinator, or may make a broader request to multiple or all CMA Coordinators. Requests for assistance may be made in response to a particular cyber emergency or in advance of a threatened or anticipated cyber emergency.

What kind of assistance is provided under the CMA Program?

In responding to a request for assistance, a participating entity's response is voluntary, intended to be advisory in nature, and provided on a short-term basis. Assistance may include services, personnel, and/or equipment.

Who is participating in the CMA Program?

Currently more than 170 entities, representing electric and natural gas investor-owned companies, public power utilities, electric cooperatives, Regional Transmission Organizations and Independent System Operators, and Canadian energy companies, participate in the CMA Program. These entities cover approximately 80 percent of U.S. electricity customers, roughly 75 percent of U.S. domestic natural gas customers, and approximately 1.25 million electricity customers in Canada.

ESCC
Electricity Subsector
Coordinating Council

For more information about the CMA Program or to become a participant, please visit www.electricitysubsector.org/CMA or contact cma@electricitysubsector.org.

January 2021

Federal Energy Regulatory Commission (FERC) Critical Energy/Electric Infrastructure Information (CEII) Regulations

Critical Energy/Electric Infrastructure Information (CEII) Regulations

The Commission has established procedures for gaining access to critical energy/electric infrastructure information (CEII) that would otherwise not be available under the Freedom of Information Act (FOIA):

- CEII is defined as infrastructure explicitly covers proposed facilities, and does not distinguish among projects or portions of projects.
- These procedures details which location information is excluded from the definition of CEII and which is included.
- The rule addresses some issues that are specific to state agencies, and clarifies that energy market consultants should be able to get access to the CEII they need.
- The rule modifies the proposed CEII process and delegates' responsibility to the CEII Coordinator to process requests for CEII and to determine what information qualifies as CEII.

Order No. 833, issued November 17, 2016
The FAST Act, signed into law by President Barack Obama in December 2015, adds section 215A to the Federal Power Act to improve security and resilience of energy infrastructure in the face of emergencies. The FAST Act required FERC to issue regulations aimed at securing and sharing CEII. Specifically, the Order includes the following amendments to the CEII regulations:

- Establishes criteria and procedures to designate information as CEII;
- Prohibits unauthorized disclosure of CEII;
- Establishes sanctions for FERC employees and certain other individuals who knowingly and willfully make unauthorized disclosures; and
- Facilitates voluntary sharing of CEII among federal, state, political subdivision and tribal authorities; the Electric Reliability Organization; regional entities; owners, operators and users of critical electric infrastructure; and other entities deemed appropriate by the Commission.

Order No. 702, issued October 30, 2007- This Order:

- Modifies non-disclosure agreements and modifies the Commission's process to allow the CEII Coordinator to respond to CEII requests by letter.
- This rule provides landowners access to alignment sheets for the routes across or in the vicinity of their properties.
- This rule includes a provision for assessing fees for requests.
- This rule limits the portions of forms and reports the Commission defines as containing CEII.
- The rule eliminates as a category of documents the Non-Internet Public designation.
- The rule provides that the Commission will seek a requester's date and place of birth on a case-by-case basis rather than require that information with every request for CEII and the request for social security numbers is being eliminated.

Order No. 683, issued September 21, 2006 - This Order:

- Clarifies CEII as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure;
- Details which location information is excluded from the definition of CEII and which is included; and
- Modifies the CEII process by requiring requesters to submit an executed non-disclosure agreement with their requests.
  - General Non-Disclosure Agreement
  - Media Non-Disclosure Agreement
  - Federal Agency Acknowledgement and Agreement

Order No. 662, issued June 21, 2005 - This Order:

- Removes federal agency requesters from the sope of the rule;
- Modifies the application of non-Internet public (NIP) treatment; and
- Clarifies obligations of requesters.

Order No. 649, issued August 3, 2004 - This Order:

- Primarily eases the burden on owners/operators of energy facilities that are seeking CEII relating to the their own facility, and

- Simplifies federal agencies' access to CEII.

These changes will facilitate legitimate access to CEII without increasing vulnerability of the energy infrastructure.

Order No. 643, issued July 23, 2003
This Order requires companies to make information directly available to the public under certain circumstances.

Order No. 630-A, issued July 23, 2003
The Commission amended Order No. 630:

- To increase the numbers of copies filed;
- Clarified the filing process for submitting CEII; and
- The instructions for requesting rehearing of the CEII Coordinator's decision

Order No. 630, issued February 21, 2003- This Order:

- Adopts the definition of critical infrastructure that explicitly covers proposed facilities;
- Does not distinguish among projects or portions of projects;
- Details which location information is excluded from the definition of CEII and which is included;
- Addresses some issues that are specific to state agencies;
- Clarifies that energy market consultants should be able to get access to the CEII they need; and
- Adopts a CEII process and delegates responsibility to the CEII Coordinator to process requests for CEII and to determine what information qualifies as CEII.

PL02-1-000, issued October 11, 2001
The September 11, 2001 terrorist attacks on America prompted the Commission to reconsider its treatment of certain documents that have previously been made available to the public through various means. The Commission removed from the public viewing certain documents, such as oversized maps, that detail the specifications of energy facilities licensed or certificated under Part I of the Federal Power Act, and Section 7(c) of the Natural Gas Act.

This page was last updated on June 12, 2020