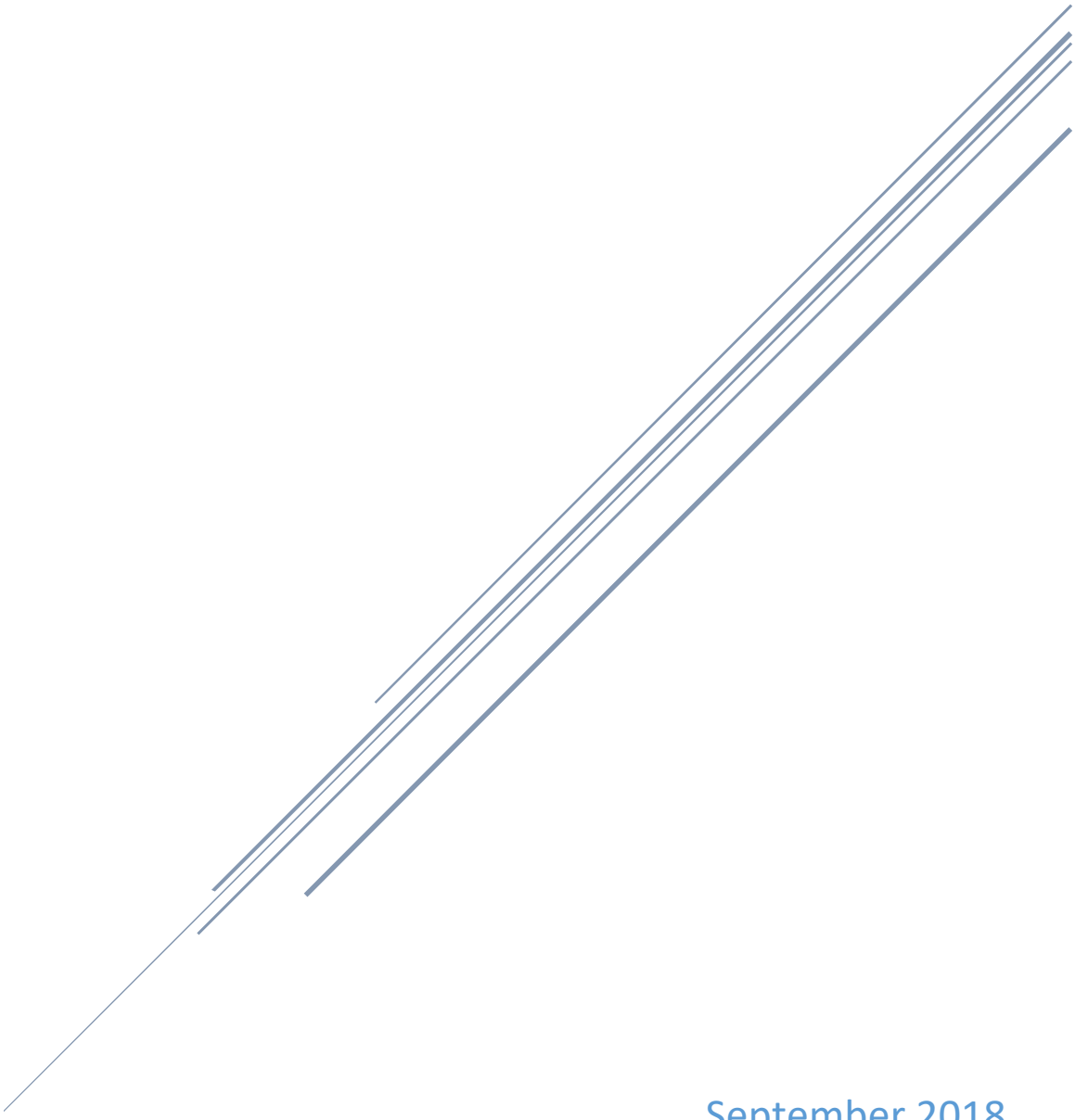
ENERGY COMMITTEE STRATEGIC PLAN

Chair: Mark Maassel | Co-Chair: Bob Richhart



September 2018
Indiana Executive Council on Cybersecurity

Energy Committee Plan

Contents

Committee Members

Committee Members

Name	Organization	Title	Committee Position	IECC Membership Type
Mark Maassel	Indiana Energy Association (IEA)	President	Chair: Full Time	Voting
Bob Richhart	Hoosier Energy	Vice President	Co-Chair: Full Time	Advisory
Scott Bowers	Indiana Electric Cooperatives (IEC)	Vice President	Full Time	Advisory
Carolyn Wright	IN Municipal Power Agency (IMPA)	Vice President	Full Time	Advisory
Kurt Aikman	Midcontinent Independent System Operator (MISO)	Manager	Full Time	Advisory
Walt Grudzinski	Vectren	Director	Full Time	Advisory
Stan Partlow	American Electric Power (AEP)/Indiana Michigan Power (I&M)	VP & Chief Security Office	Full Time	Advisory
Curtis Taylor	Wabash Valley Power Authority (WVPA)	VP, Technical Services	Full Time	Advisory
Scott Berry	IMPA	Manager, Environmental & NERC Compliance	Full Time	Advisory
Greg Ellis	Indiana State Chamber	VP	Full Time	Advisory
Paul Mitchell	Energy Systems Network (ESN)	President	Full Time	Advisory
Brain Rockensuess	Indiana Department of Environmental Management (IDEM)	Chief of Staff	As needed	Advisory
Sarah Freeman	Indiana Utility Regulatory Commission (IURC)	Commissioner	As needed	Voting Proxy
Jennifer deMedeiros	AES/ Indianapolis Power & Light (IPL)	Manager	As needed	Advisory
Allen Brown	Midwest Natural Gas	Director	Contributing	Advisory
Carl Cahill *	Duke Energy	Director	Contributing	Advisory
Chad Connell	MISO	Manager	Contributing	Advisory
Scott Miller	Citizens Energy Group	Manager	Contributing	Advisory

- Carl retired in early 2018 but was a Contributing Member of the Committee until he retired.

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**
  - 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).
  - Needs for training by educational institutions to provide cybersecurity professionals
  - Level of interaction, and need for interaction, with other subsectors'
  - 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.
  - There is in place at the national level an Electric Subsector Coordinating Council and an Oil & Natural Gas Subsector Coordinating Council. Both are quite active.
  - Electric ISAC and Downstream Natural Gas ISAC are active.
  - Significant need for education and training exists.
  - There is a need to interact with other subsectors, including for example Telecommunications and Financial.
  - The Energy Committee believes a much clearer understanding of state priorities and responses in a cyber emergency would be important.

- **Committee Deliverable**
  - Critical Infrastructure Information Training
  - Contacts
  - Coordinate with Others
  - Metrics

- **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 economy and well-being of Hoosiers, indeed for Americans. This industry is also heavily regulated, including in the cybersecurity arena. 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 the training and exercise activities in which the industry participates is Grid-Ex. Grid-Ex is a biannual, nation-wide exercise which provides utilities a chance to "experience" a cyberattack. In 2017, the exercise included both electric and natural gas utilities as well as cyber and physical attacks.
    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 also includes downstream natural gas distribution companies such as those 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. Need to improve communications between sectors on such things as threats which are detected by another sector.
    c. A common clearinghouse which assesses vendors with differing levels of cyber exposure and risk mitigation.
    d. Potential disruptions of the telecommunications networks.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. There is a significant 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). TSA has in place Pipeline Security Guidelines and is working with the industry to revise and update these guidelines.

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. These are named Grid-Ex. Grid-Ex IV was conducted in November 2017. It involved the electric and natural gas industries and tested responses to a cyberattack.

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 all required to meet the same regulations or guidelines, training in the energy industry is reasonably similar across the country. And, as noted above, in addition to more localized exercises, energy utilities engage in national exercises as well.

8. **What does success look like for your area in one year, three years, and five years?**
    a. One Year
        1. Obtain a clearer understanding of state priorities in an emergency, including how the Public Sector plans to allocate scarce resources.
        2. Further development of curriculum at Indiana educational institutions to develop individuals for employment in cybersecurity.
        3. Development of a process to share threat information across and between sectors.
    b. Three Years
        1. Utilities have, if needed, modified plans to reflect Public Sector priorities.
        2. Utilities can begin to hire well trained and educated cybersecurity professionals.
        3. Robust information sharing processes have become standard operating procedure.
        4. Appropriate involvement of others on the Council in Grid-Ex, including observers.

c. Five Years
    1. Ongoing evolution of the way we work together in Indiana has revised and changed the way we work as we respond to the ever-changing risk environment.
    2. Utilities have an ever-increasing number of graduates from Indiana educational institutions who can 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. As mentioned above, Indiana's educational institutions should be more intentional about training students for cybersecurity roles. Increased awareness of the importance of these roles and the types of jobs available in the field is needed.

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

a. Total Workforce
    - Over 12,000 direct employees.

b. Cybersecurity-related workforce
    - Over 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. We will be better able to provide thoughts on this issue once we learn more about what already exists in the other sectors. Clearly, 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 seem, at least on a preliminary basis, as an area ripe for implementation.

Deliverable: Critical Infrastructure Information (CII)

Deliverable: Critical Infrastructure Information

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?**
    a. 100 % Complete

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 Energy Committee is aware of the numerous existing rules and guidelines which already impact how electric and natural gas energy companies address cyber issues. Additional laws, regulations or policies will certainly increase the work required, potentially without increasing cybersecurity and with the potential to create conflicting laws, regulations or policies. We do not believe that additional laws or policies are needed in Indiana. We will monitor this issue since others may have ideas that warrant review by this Committee.

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?**
    a. 2018
    b. Rules have been in place for Indiana's energy sector members for almost 10 years.

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

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 put in place mandatory regulations and/or guidelines which impact companies across the nation as well as here 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 the pervasive use of electricity and natural gas by almost all Hoosiers, 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 Mark Maassel at the Indiana Energy Association. It is his 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. We believe that the only challenge, with consideration the IECC is set up in a manner that helps address the challenge, is the flow of information between and among IECC Committees and/or Working Groups.

Implementation Plan

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

a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Critical Infrastructure Information (CII) in the energy industry is defined by federal entities.	FERC and the TSA	100%	Complete	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
No additional staffing is required					

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 is 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 rise 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 into the future.

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

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. 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?

a. Yes
b. 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)?

a. Yes

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

a. While others are much better positioned and informed to answer this question, we do not necessarily see this item as a key for either public relations or marketing consideration.

Evaluation Methodology

Objective 1: IECC Energy Committee will provide current definitions and review of potential policy changes to protect critical infrastructure information while maintaining public access and freedom of information by July 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Deliverable: Training

Deliverable: Training

General Information

1. **What is the deliverable?**
    a. Determine the need to establish a training program.

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

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 this industry needs in training and education to support and enhance energy company cybersecurity.

6. **What metric or measurement will be used to define success?**
    a. This is likely best done by committee/task force that is focused on these issues. We are prepared to support their efforts as needed. The Workforce Development Committee responded to a question from this Committee that they will propose the formal adoption of the NICE framework by the IECC. This Committee supports the adoption of the NICE framework.

7. **What year will the deliverable be completed?**
    a. 2023+
    b. We would hope for progress in each of the upcoming years but acknowledge that the industry is evolving rapidly, and educational efforts will also be changing.

8. **Who or what entities will benefit from the deliverable?**
    a. All aspects of those involved directly in cybersecurity will benefit from an increasing pool of talented cyber experts, including organizations outside of Indiana.

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. We will support other committees/working groups as they develop their plans. We anticipate that all committees of the Council will need to be a part of defining what is needed to train individuals to work in cybersecurity.

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. This will be best defined by the Committees and Working Groups who are directly developing the needed training.

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Mark Maassel at the Indiana Energy Association. It is his 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?**
    a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
The Energy Committee believes that a training program with certifications as well as college level and advanced degrees, providing initial and ongoing reskilling opportunities is needed. This should be focused around the NICE standards.	Workforce Development Committee	100% (The Energy Committee work of identifying the need is complete. We are prepared to support the Workforce Development Committee as they proceed forward.) [1]	Complete	
Develop and promote Certified Hacker Training Program.	Workforce Development Committee	100% (The Energy Committee work of identifying the need is complete. We are prepared to support the Workforce Development Committee as they proceed forward.) [1]	Complete	
Develop apprenticeship programs to help individuals who are entering the Cybersecurity field develop their skills and gain "real world" experience.	Workforce Development Committee	100% (The Energy Committee work of identifying the need is complete. We are prepared to support the Workforce Development Committee as they proceed forward.) [1]	Complete	
When individuals first begin to receive training, teach secure coding early on, perhaps even before teaching coding.	Workforce Development Committee	100% (The Energy Committee work of identifying the need is complete. We are prepared to support the Workforce Development Committee as they proceed forward.) [1]	Complete	

[1] The IECC Energy Committee is comprised of a wide array of entities providing electric and natural gas services in Indiana. Walt Grudzinski who serves on the Energy Committee and the Workforce Development Committee will serve as the key contact point for questions and further input which Workforce Development may require from the Energy Committee. In addition, the Committee has determined that Mark Maassel should be the back-up contact point for questions and further input as needed by the Workforce Development Committee. He will engage the appropriate resources to support the Workforce Development Committee

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
Minimal	Minimal	Supervisory experience which informs the individual on the training required to function in cybersecurity roles inside the energy industry.	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. This will provide a skilled pool of applicants ready to address cybersecurity issues from which the energy industry can draw to staff our workforce.

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 here in Indiana.

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

a. Most likely the industry will hire individuals from outside of Indiana. It will be a missed opportunity for Hoosiers to learn and develop the skills needed.

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

a. The Energy Committee believes these are better developed by the Workforce Development Committee. For us, success is simply having Hoosiers who possess the skills the energy industry needs as we look to fill openings in our staff.

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

a. Yes
b. Virginia has a program which warrants review by the IECC.

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. Any state other than those listed in response to question 21 may be a potential control.

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?

a. No

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

a. The Workforce Development Committee is best suited to address this issue.

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

a. In responses to the questions asked in Phase 1, we have alerted the Workforce Development Committee of our needs.

27. Can this deliverable be used by other sectors?

a. Yes
b. 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)?

a. Yes

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

a. Others are better positioned and informed to address this issue. However, it would seem to be a wonderful opportunity to highlight the capabilities of Indiana's educational system and the ability to "tune" that system to train individuals in a new, developing set of skills needed in the workplace.
b. Just to reiterate, the IECC Energy Committee recognizes that we will need to engage in an ongoing, bi-directional dialog with the Workforce Development Committee and others to assure that the appropriate training and education is being provided to those entering the field. This will be critical given the rapidly changing cyber environment and the need for flexibility and adaptability to meet the challenges and seize the opportunities presented by these changes.

Evaluation Methodology

Objective 1: IECC Energy Committee will provide the IECC Workforce Development Committee the needs of the energy sector, as well as examples to consider as Indiana cybersecurity training and apprenticeship programs, are being developed by July 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Deliverable: Contacts

Deliverable: Contacts

General Information

1. **What is the deliverable?**
    a. Identify energy companies within the State of Indiana, form of ownership and how cyber is managed. Develop and maintain a critical contact database.

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

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. Appropriate contact information is available in the event of a cyberattack.

6. **What metric or measurement will be used to define success?**
    a. This will be measured by the existence of a contact list and its updating. The updates will be done by the IURC. The survey will be used to verify, among other things, contact information.

7. **What year will the deliverable be completed?**
    a. 2018
    b. An initial list will be developed in 2018. However, this will need periodic updating and will never be finished.

8. **Who or what entities will benefit from the deliverable?**
    a. All individuals and organizations who are a part of the protection against cyberattacks or in recovering from cyberattacks.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. We are not aware of any overlap on this issue.

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 this deliverable does not require input from other IECC Committees and/or Working 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. The IURC will be the central point for the collection of the information. The IURC and the IDHS will be involved since they will be the central points in a cyber emergency.

12. **Who should be main lead of this deliverable?**
    a. The IURC leads the effort to assemble the contact information. In addition, the Energy Committee is structured so that information flows to Mark Maassel at the Indiana Energy Association. It is his 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. We do not anticipate major challenges to completing this deliverable.

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
On a routine basis, survey the Indiana energy utilities to determine the appropriate contacts for cyber issues.	The Indiana Utility Regulatory Commission already gathers critical contact information for physical events which impact the operations of electric and natural gas utilities. They will expand this information gathering and updating to include cyber contacts.	Completed	June 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
Less than 1	Less than 1		Cost will be covered by each respondent and the IURC	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. Assure the existence of up-to-date contact information.

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

a. Up-to-date contact information will assist in more timely and responsive communications planning, testing and recovery.

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

a. Less than ideal exchange of information and ideas in planning, testing and recovery.

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

a. Responses to the request for up-to-date contact information will define success.

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

a. Most other states collect this type of information.

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. The Energy Committee is unaware of any state that does not gather such information.

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?

a. No

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

a. Needed personnel and other resources are in place.

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

a. Committee discussions have identified the IURC as the best-positioned entity to gather the needed information.

27. Can this deliverable be used by other sectors?

a. Yes
b. This approach could work for any sector which might be planning for, testing or involved in recovery from a cyber incident would benefit. Other approaches might work for them as well. We selected this approach as a practical and effective mechanism in the energy industry.

Communications

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

a. Both the IURC and IDHS will need and want this information. This follows the existing practices for the IDHS Emergency Operations Center and will simply be expanded to include both contacts for physical interruptions of service as well as cyber interruptions.

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

a. No

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

a. While others are much better positioned and informed to answer this question, we do not necessarily see this item as a key for either public relations or marketing consideration.

Evaluation Methodology

Objective 1: Over eighty-five percent of Indiana electric and natural gas utilities provided the Indiana Utility Regulatory Commission's Emergency Support Function lead on behalf of Indiana Department of Homeland Security a cybersecurity contact by June 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: The Indiana Utility Regulatory Commission's Emergency Support Function lead will maintain the cyber contact list on behalf of the Indiana Department of Homeland Security Emergency Operations Center annually.

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: Coordinate with Others

Deliverable: Coordinate with Others

General Information

1. **What is the deliverable?**
    a. Coordinate with Working Groups as appropriate.

2. **What is the status of this deliverable?**
    a. While the work of coordinating with others will be an ongoing process, for the first year the Energy Committee has completed this deliverable.

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. We have supported the work of other sectors as well as achieved an appropriate level of sharing of information and risks through existing channels such as the E-ISAC. The Energy Sector will continue to share information through these types of channels. From there, information should be shared through a Multi-sector ISAC.

6. **What metric or measurement will be used to define success?**
    a. Because energy sector companies already follow the rules and guidelines established by the NERC and TSA, the sector has strong cyber plans and processes in place. The Indiana Energy Association (IEA) will conduct an annual survey of the energy sector asking questions to measure the status of cyber preparedness. They are:
        i. Do you have a plan?
        ii. If so, do you review and exercise the plan periodically?

7. **What year will the deliverable be completed?**
    a. 2018. The survey was conducted in May and June. Final results were sent to the IECC on June 2018. The results are also attached as Supporting Documentation.
    b. The IECC final report will serve as the completion of this deliverable.

8. **Who or what entities will benefit from the deliverable?**
    a. Done correctly, all participants will benefit.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. We are not aware of an overlap at the moment; however, recognize that the potential for overlap grows as both federal and state government move ahead with various initiatives

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 cybersecurity is best advanced by using the existing infrastructure. Specifically, each sector should continue to work with their ISAC who in turn should work with the multi-sector ISAC. State of Indiana contacts should be coordinated through IDHS. IDHS can work with the IURC for energy sector contacts.

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. Our experience with Subsector Coordinating Councils has been positive. The entities who make up these Councils are the individuals and organizations who need to be involved. From the standpoint of other sectors (e.g., the Financial Sector) we are hopeful that the correct individuals and organizations are engaged. Thus, the issue is more about opening lines of communications between the Councils. Furthermore, state-based associations like the IEA will be available to IDHS.

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Mark Maassel at the IEA. It is his 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. We are not aware of any challenges at this point.

Implementation Plan

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

a. One-time deliverable

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Support others as appropriate	Energy Committee	100%	May 2018	
Respond to questions asked by other Committees & Working Groups	Energy Committee	100%	November 2017	
Provide appropriate information to the Energy ISAC. We hope to receive information which we can act upon from other ISAC's through a cross-sector ISAC.	Energy Committee	100% though ongoing. This is built into our existing processes.	May 2018	
Provide a contact to Chetrice Mosely for an individual at the North American Electric Reliability Council so she can assess whether such a speaker should present to the IECC or at the Cyber Summit.	Stan Partlow	100%	June 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
No additional staff is required.					

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. The development of a cohesive cyber plan for Indiana which does not create unwarranted requirements on time or funds which do not enhance cybersecurity and preparedness.

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

a. Better coordination of efforts and of information exchanges will reduce cybersecurity risk and impact. The costs are all a part of the existing business costs for the energy utility industry.

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

a. A less cohesive cyber plan for Indiana.

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

a. Success will be shown by working with other Committees and Working Groups effectively.

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, we are not aware of any.

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, we are not aware of any.

Other Implementation Factors

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

a. We are not aware of any.

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 communications designed to enhance cybersecurity are welcome.

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

a. We have, through the questionnaire completed in November 2017, reached out to several committees and responded to their questions.

27. Can this deliverable be used by other sectors?

a. Yes
b. We would assume that all Committees and Working Groups are supportive of communicating to enhance cybersecurity in Indiana.

Communications

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

a. All stakeholders can be informed that the energy utility industry and this Committee are willing to work with others to support enhancing cybersecurity in Indiana.

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

a. Yes, assuming that there are no confidentiality or security concerns with the information.

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

a. While others are much better positioned and informed to answer this question, we do not necessarily see this item as a key for either public relations or marketing consideration.

Evaluation Methodology

Objective 1: IECC Energy Committee will coordinate with other committees and working groups as needed to effectively complete the State Cybersecurity Strategic Plan by September 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Objective 2: IECC Energy Committee will share information with Energy ISAC regarding Indiana's new cyber sharing resources 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

Deliverable: Metrics

Deliverable: Metrics

General Information

1. **What is the deliverable?**
    a. Establish metrics to assess the overall risk to the State of Indiana regarding Energy utility operations.

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

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 goal is to establish accountability and clarity of the effectiveness of cybersecurity programs and response plans. Energy sector companies already follow the rules and guidelines established by NERC and TSA, the sector has strong cyber plans and processes in place. The IEA will conduct an annual survey of the energy sector asking questions to measure the status of cyber preparedness. They are:
        i. Do you have a plan?
        ii. If so, do you review and exercise the plan periodically?

6. **What metric or measurement will be used to define success?**
    a. Metrics are in place inside the energy industry with which the companies comply. As Indiana develops its metrics, we will seek to dovetail existing metrics used in the energy industry into the Indiana framework without creating unnecessary work. This has been accomplished with the creation of the survey described in Question 5.

7. **What year will the deliverable be completed?**
    a. 2018
    b. Indiana's electric and natural gas energy industry responded to the survey which was developed to assure that effective cybersecurity planning is in place in the energy industry and help to advance cybersecurity.

8. **Who or what entities will benefit from the deliverable?**
    a. Generally speaking, metrics provide valuable insights into planning and execution of the measures taken to address cyber risks.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. We do not believe there is any overlap at the moment. The risk will be that the Indiana specific metrics do not recognize the existing federal requirements creating added work which might detract from addressing cyber issues.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Coordination with the Strategic Resource Task Force will be important.

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. This work will largely flow from the ongoing engagement with federal agencies. Key among these are DHS, TSA, FERC and NERC.

12. **Who should be main lead of this deliverable?**
    a. The Energy Committee is structured so that information flows to Mark Maassel at the IEA. It is his 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. Assuring adequate flow of information to other committees/task forces and a similar flow from them to the Energy Committee.

Implementation Plan

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

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
The IECC Energy Committee developed a set of two questions which can be asked annually to assess planning, preparedness and recovery in the utility energy industry.	This will be coordinated by the IEA and provided to the IECC.	100%	June 2018	Given the pervasive nature of federal requirements, relatively few questions and one metric are needed to assess the status of the energy industry in Indiana.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
No additional staff is required.					

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. Though pervasive federal regulation and guidance of cyber issues exists in the energy utility arena, this will provide a metric to quickly and effectively relay the status to Indiana stakeholders.

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

a. The metric will quickly identify the situation here in Indiana. It should be noted that a reduction in cyber risk is already achieved through the federal regulation and guidance which is in place. This metric will help in communicating a complex set of rules and their application in a highly specialized, technical industry to those in Indiana who seek to understand the status of this industry.

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

a. The vast majority of cybersecurity in the energy utility industry results from existing federal regulations and guidance.

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

a. Responsiveness of energy utility industry participants will be a measure of success. The baseline was established when the first ever survey was sent to the industry. One hundred percent of those surveyed responded to the survey providing a comprehensive look at the planning that exists within the Indiana energy utility space.

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. We are not aware of any.

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. We are not aware of any.

Other Implementation Factors

---

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

a. We are not aware of any.

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. See the "Owner" column in the "Tactic Timeline" table above.

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

a. This was developed by the Energy Committee.

27. Can this deliverable be used by other sectors?

a. Yes

b. This may be applicable to and useful for other sectors. However, the metric was developed with an eye to the existing regulations and guidelines which the energy utility industry follows. We believe that the level of existing regulation and guidelines are unique to this industry.

Communications

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

a. The Indiana Executive Cybersecurity Council. The results of the survey are attached as a part of the Supporting Documentation.

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. While others are much better positioned and informed to answer this question, we do not necessarily see this item as a key for either public relations or marketing consideration.

Evaluation Methodology

Objective 1: IECC Energy Committee will provide the utility energy industry an annual survey that will assess cybersecurity planning, preparedness and recovery posture by June 2018. A summary of the results from all those who were surveyed was sent to the IECC.

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: Eighty percent of all utilities will complete annual survey by July 2018. The actual result was one hundred percent participation with all responses received prior to June 2018.

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Supporting Documentation

Supporting Documentation

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

- American Public Power Association (APPA) – Cybersecurity and the Electric Sector
- Electricity Subsector Coordinating Council (ESCC) Brochure
- Federal Energy Regulatory Commission (FERC) Critical Energy/Electric Infrastructure Information (CEII) Regulations
- IECC Energy Committee Annual Metrics Report
- IECC Energy Committee Commonwealth of Virginia (CoV) Briefing
- National Conference of State Legislatures (NCSL) – State Efforts to Protect the Electric Grid

American Public Power Association (APPA)

Cybersecurity and the Electric Sector

June 2017

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

ISSUE BRIEF June 2017

Cybersecurity and the Electric Sector

Summary

The electric utility industry (including public power utilities) takes very seriously its responsibility to maintain a strong electric grid and it is the only critical infrastructure sector besides nuclear power that has any mandatory and enforceable federal regulatory standards in place for cybersecurity. As the grid evolves, unfortunately, so do threats to its integrity. The threat of cyber-attacks is relatively new compared to long-known physical threats, but an attack with operational consequences could occur and cause disruptions in the flow of power if malicious actors are able to hack into data overlays used in some electric generation and transmission infrastructure. Furthermore, such an attack could also cause public power utilities to incur liability for damages. While the American Public Power Association (Association or APPA) believes that the industry itself, with the North American Electric Reliability Corporation (NERC), has made great strides in addressing cybersecurity threats, vulnerabilities, and potential emergencies, it recognizes that emergency situations warranting federal involvement may arise.

Background and Congressional Action

The electric utility sector is the only critical infrastructure sector besides nuclear power plants (a part of the overall sector) that has any 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 (Section 215 of the Federal Power Act). Under Section 215, NERC, working with electric industry experts, regional entities, and government representatives, drafts reliability and cybersecurity standards that apply across the North American grid, inclusive of Canada. Participation by industry experts and compliance personnel in the NERC 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, NERC conducts 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.

To date, the electric utility sector's Federal Power Act (FPA) Section 215 processes and its actions beyond the Section 215 regime have prevented a successful cyber-attack causing operational consequences on the bulk electric system in the United States. That said, APPA 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, the Association strongly supported passage of the Cybersecurity Act of 2015, which was incorporated as Division N of H.R. 2029, the Consolidated Appropriations Act, 2016. The Act set up policies and procedures for sharing cybersecurity threat information between the federal government and private entities (which include public power) and between private entities and provides limited liability protection for these activities if conducted in accordance with the Act.

In addition to the Cybersecurity Act of 2015, the Association strongly supported Section 61003 of P.L. 114-94 (the "FAST Act"), which gave the Secretary of Energy broader authority to address grid security emergencies under the FPA and 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. Specifically, the provision directed that FERC-designated CEII be exempt from disclosure for a period of up to five years with a process to lift the designation or challenge it in court and established sanctions for the unauthorized disclosure of shared information. FERC issued a final rule to implement this provision on December 21, 2016.

Outside of the legislative process, the Association and its members, as well as other utilities, continue to participate in the NERC Critical Infrastructure Protection (CIP) standards drafting process on cyber and physical security. (See APPA's "Physical Security and the Electric Sector" issue brief for more information on the physical-security standard.) As attacks on critical electric infrastructure are ever-changing, so must be the nature of our defenses, whether they are designed to protect cyber or

physical assets. As such, CIP Version 5 are in effect and became enforceable on July 1, 2016.

APPA is also involved with internal and external working groups to enhance the security of the electric grid. The Association and its members play a leadership role in the Electricity Subsector Coordinating Council (ESCC), the government/industry partnership focused on security and information sharing that is mentioned earlier in this document. Through the ESCC, APPA works with the other critical infrastructure sectors, such as the downstream natural gas and dam sectors.

Administrative Action

On May 11, 2017, President Trump signed a long-anticipated Executive Order (EO), "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The EO states that "It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure." It directs the Department of Energy (DOE), Department of Homeland Security, and Director of National Intelligence, along with other stakeholders, to assess within 90 days: "(i) the potential scope and duration of a prolonged power outage associated with a significant cyber incident against the United States electric subsector; (ii) the readiness of the United States to manage the consequences of such an incident; and (iii) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident." APPA is still reviewing the EO and will provide additional analysis as necessary. President Trump's EO builds on the one issued by former President Obama in February 2013 requiring the creation of a cybersecurity framework, which was subsequently released by the National Institute for Science and Technology (NIST) in February 2014. The Association has strongly encouraged its members to adopt this framework and evaluate their cybersecurity plans.

Finally, the Association has also partnered directly with DOE. APPA and DOE signed a three-year Cooperative Agreement in 2016 for up to $2.5 million per year to accelerate the Association's efforts to help its members understand and implement resiliency, cybersecurity, and cyber-physical solutions, including refining and improving the adoption of advanced control concepts. We respectfully encourage Congress to continue fully funding research in this area through DOE's Office of Electricity Delivery and Energy Reliability (OEDER).

American Public Power Association Position

Protecting the cybersecurity of the electric grid is of upmost importance to public power utilities and the electric utility industry as a whole. The regulations and standards ("NERC-FERC") process set up in the 2005 Energy Policy Act continue to 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, we recognize that we 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 and, as such, will continue to invest considerable resources into this effort.

American Public Power Association Contacts

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

Cory Toth, Government Relations Director, 202-467-2939 / ctoth@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)

Brochure

November 2017

NOVEMBER 2017

ESCC

Electricity Subsector Coordinating Council

Protecting the energy grid from threats that could impact national security is a responsibility shared by both the government and the electric power sector.

The Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the federal government and the electric power industry, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC includes electric company CEOs and trade association leaders representing all segments of the industry. Its counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

Background

In October 2010, the National Infrastructure Advisory Council (NIAC) issued a report, *A Framework for Establishing Critical Infrastructure Resilience Goals*, that included nine recommendations. The first recommendation was:

> **NIAC Recommendation:** "The White House [will] initiate an executive-level dialogue with electric and nuclear sector CEOs on the respective roles and responsibilities of the private sector in addressing high-impact infrastructure risks and potential threats... ."

This recommendation was the impetus for initial meetings in July 2012 between an ad hoc group of industry CEOs and Department of Energy (DOE) Secretary Steven Chu and Department of Homeland Security (DHS) Secretary Janet Napolitano. These meetings resulted in a classified briefing for the industry in September 2012 and led to the formation of the Joint Electric Executive Committee, which was convened in January 2013 and which had a commitment to meet quarterly with the Deputy Secretaries of DOE and DHS.

Ultimately, the Joint Electric Executive Committee transitioned to its current official role as the ESCC.

ESCC Areas of Focus

Industry and government leaders have agreed to focus on four main areas that improve the security posture of the industry and the nation. To support the deployment of tools, improve the flow of threat information, prepare for incidents, and work closely with other interdependent infrastructure sectors, the ESCC has organized into strategic committees with the following missions:

Threat Information Sharing: Improve and institutionalize the flow of, and access to, actionable information among public- and private-sector stakeholders.

Industry-Government Coordination: Establish unity of effort and unity of messaging between industry and government partners to support the missions of the ESCC both during crises and in steady state.

Research & Development: Coordinate government and industry efforts on strategic infrastructure investments and R&D for resilience and national security-related products and processes.

Cross-Sector Liaisons: Develop strong partnerships at all levels of the Electricity, Communications (Telecommunications), Oil and Natural Gas (Downstream Gas), Financial Services, Transportation Systems, and Water and Wastewater Systems (Water) sectors to plan and respond to major incidents, to better understand and protect our mutual dependencies, and to share information effectively and efficiently to improve cross-sector situational awareness.

Security Executive Working Group

To support the mission of the ESCC, a Security Executive Working Group (SEWG) convenes by phone on a monthly basis and creates ad hoc teams to accomplish the goals identified by the CEOs and Deputy Secretaries. In parallel to this effort, the government also has organized around these goals with a commitment to align government and industry efforts.

ESCC Official Roster

November 2017

Leadership (3)

Tom Fanning, Southern Company (co-chair)
Kevin Wailes, Lincoln Electric System (co-chair)
Duane Highley, Arkansas Electric Cooperative (co-chair)

Steering Committee (9)

Sue Kelly, American Public Power Association
Sergio Marchi, Canadian Electricity Association
Tom Kuhn, Edison Electric Institute
John Shelk, Electric Power Supply Association
Andrew Ott, PJM (representing the ISO/RTO Council)
Mike Wallace, National Infrastructure Advisory Council
Jim Matheson, National Rural Electric Cooperative Association
Gerry Cauley, North American Electric Reliability Corporation
Maria Korsnick, Nuclear Energy Institute

Asset Owners
(19: 13 investor-owned electric companies; 3 electric cooperatives; 3 municipal electric companies)

Nick Akins, American Electric Power
Jim Torgerson, Avangrid
Scott Miller, City Utilities of Springfield
John McAvoy, Consolidated Edison
Tom Farrell, Dominion
Lynn Good, Duke Energy
Pedro Pizarro, Edison International
Gianna Manes, ENMAX Corporation
Chris Crane, Exelon Corporation
Greg Ford, Georgia System Operations Corporation
David Saggau, Great River Energy
Connie Lau, Hawaiian Electric Industries
William Fehrman, MidAmerican Energy Co.
John Bilda, Norwich Public Utilities
Jack Reasor, Old Dominion Electric Cooperative
Tony Earley, PG&E Corporation
Bill Spence, PPL Corporation
Gil Quiniones, New York Power Authority
Ben Fowke, Xcel Energy

ESCC Coordination

Coordination among senior government and industry executives helps to ensure an effective response, appropriate prioritization and allocation of resources, and support for deviation from standard procedures during an incident.

ESCC Stakeholders

Government

- Federal Agencies
- Regulators
- PMAs
- Law Enforcement
- State, Local, Tribal, & Territorial
- Canadian Agencies & Provinces

Industry

- Electric Companies
- Trade Associations
- ISOs & RTOs
- NERC
- E-ISAC
- Canadian Electric Companies

External Groups

- Other Critical Sectors
- Vendors
- Critical Customers
- Media

Coordination

- Security to support restoration
- Media and public affairs messaging
- Logistical support, staging

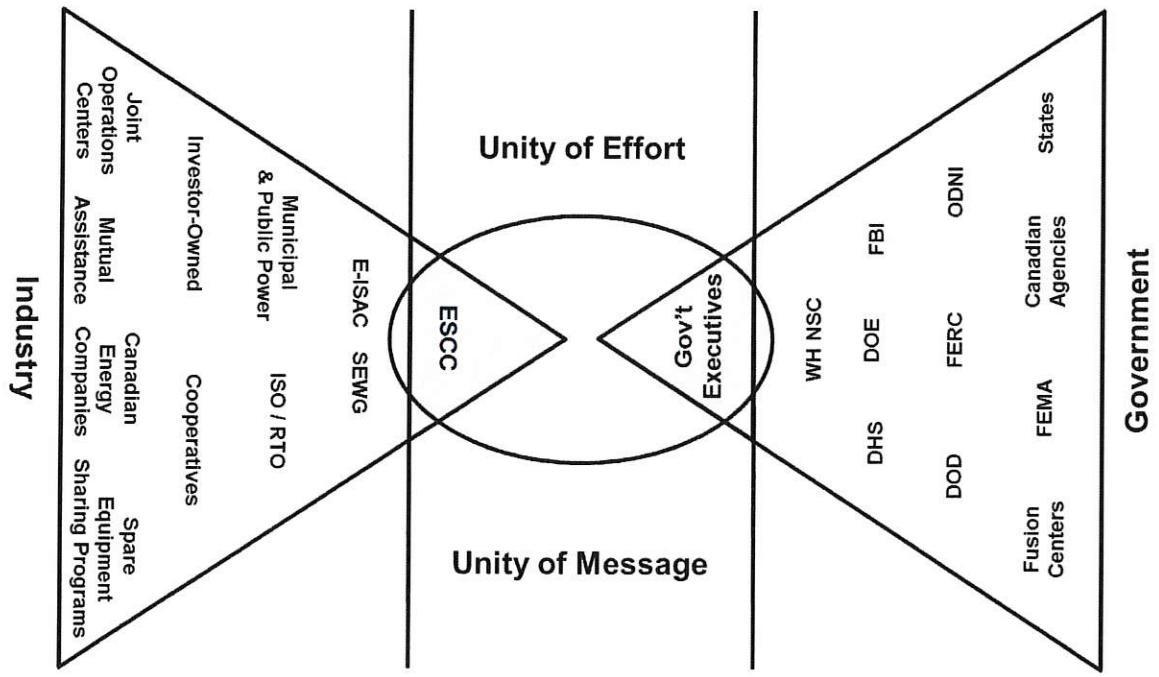
Resource Allocation

- Equipment, hardware, and materials
- Human resources and expertise

Conflict Resolution

- Investigation versus restoration
- Prioritization of recovery
- Distribution of limited resources

Industry-Government Coordination



ESCC Member Structure

Electricity Subsector Coordinating Council (ESCC)

Electricity Information Sharing and Analysis Center (E-ISAC)

Leadership

Co-chairs representing the three major industry segments

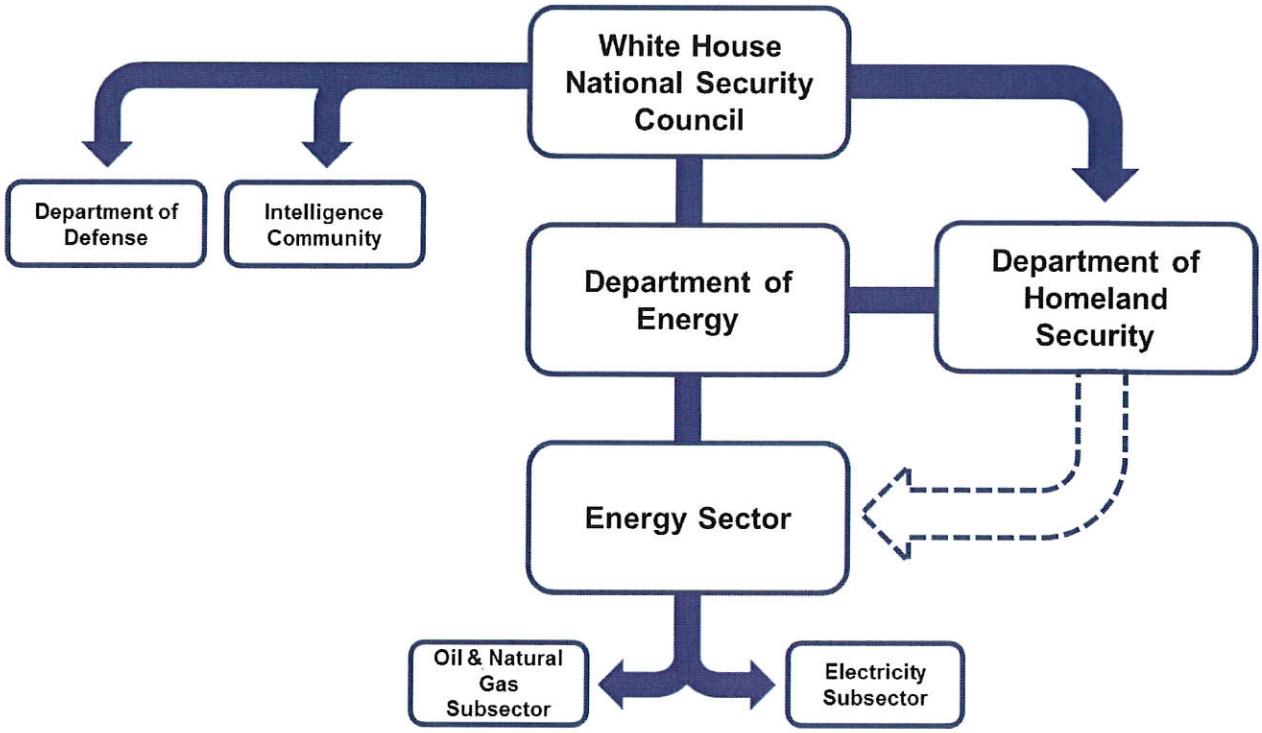
Steering Committee

NIAC representative, APPA, CEA, EEI, EPSA, ISO/RTO Council, NEI, NERC, and NRECA

Asset Owners

CEOs proportionally representing asset owners from across industry segments

Energy Sector-Government Organizational Structure



ESCC
Electricity Subsector Coordinating Council

Federal Energy Regulatory Commission (FERC)

Critical Energy/Electric Infrastructure Information (CEII) Regulations

November 2016

FERC Federal Energy Regulatory Commission

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 PDF, 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 PDF, 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.

IECC Energy Committee

Annual Metrics Report

June 2018

Indiana Executive Cybersecurity Council

Energy Committee

Annual Update and Measurement of Metrics

2018

Company	Do you have a plan?	Do you review and exercise the plan periodically?
Citizens Energy Group	Yes	Yes
Duke Energy	Yes	Yes
Hoosier Energy	Yes	Yes
IMPA	Yes	Yes
IN MI Power/AEP	Yes	Yes
IPL/AES	Yes	Yes
MISO	Yes	Yes
NIPSCO	Yes	Yes
Vectren	Yes	Yes
WVPA	Yes	Yes

IECC Energy Committee

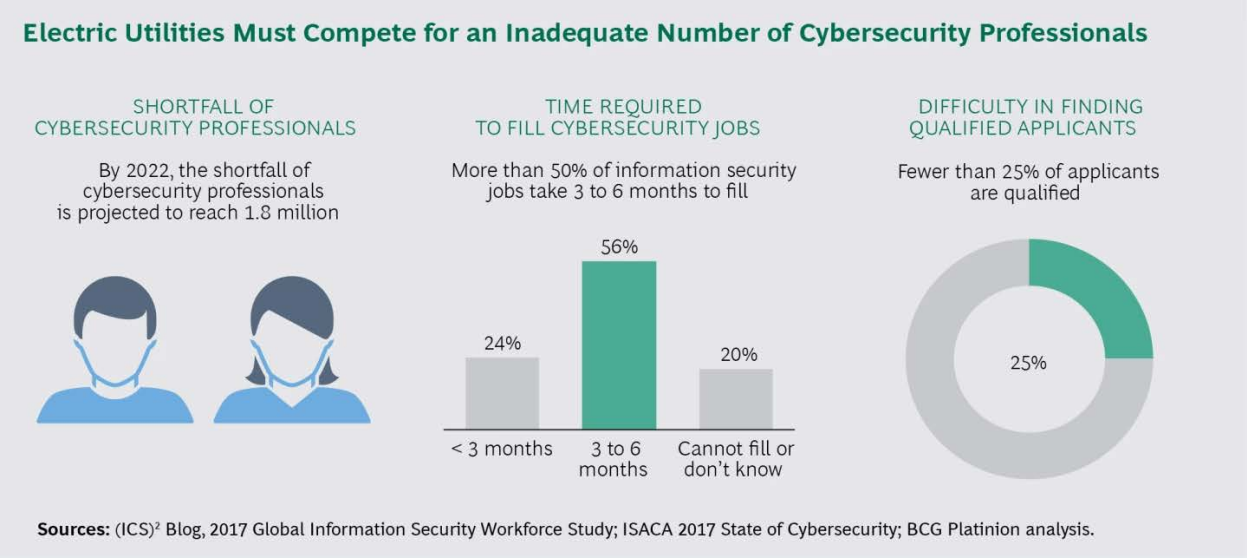
Commonwealth of Virginia (CoV) Briefing

May 2018

TO: Mark Maassel, Indiana Energy Association President
CC: Energy Working Group, Indiana Executive Council on Cybersecurity
FROM: Jennifer de Medeiros, Infrastructure Security Analyst, AES Corp.
RE: Cyber Workforce Training Standards & Standardbearers

Given the pace of technological change and rapidly sophisticating threat landscape, the State of Indiana is challenged to grow and retain a skilled workforce that can continuously evolve alongside the cyber ecosystem. The Commonwealth of Virginia is regarded as having set the standard for a diversified training portfolio that targets a cross-section of residents, including traditionally underserved populations. It is recommended that the IECC consider similar avenues that can offer targeted training opportunities for strongly needed professional functions within the critical infrastructure sectors.

This is especially important for the energy industry, which has a unique need for not only information technology (IT) and operations technology (OT) professionals, but professionals who can navigate both systems. Given the complexity of securing both IT and OT systems, utilities in particular suffer from a shortage of professionals who can address cybersecurity needs. Teaching IT professionals about OT—and OT professionals about IT—is not always easy or effective. Education and training organizations should continue to focus on developing converged IT-OT cybersecurity practitioners using a variety of methods.



Indiana should support cyber programs at community colleges, and support accreditation as National Centers of Academic Excellence. Indiana is well known for its excellent higher education cyber programs at Purdue, Indiana University, IUPUI and others. However, these programs may be outside the reach of many Hoosiers due to their cost and length. In Virginia, there are 62 Centers of Excellence, 5 of which are 2-year community colleges. Offering more options – including converged IT-OT training options – for Hoosiers of all income levels will ensure cybersecurity is sewn into the fabric of our education system.

Apprenticeship programs are a proven method for filling talent gaps and accelerating learning – without the cost of formal education. Because there are so few formal educational opportunities for the IT-OT system, utilities and energy partners must offer hands-on, tacit learning experiences to train their own personnel and facilitate knowledge transfer within the industry. It is not easy to educate IT professionals in an OT environment, and vice versa. Cybersecurity apprenticeships can be particularly effective in

navigating in this unique environment, which typically has a technological “reset” of seven years. Apprentice programs also accelerate learning without the cost of long-term formal education programs.

- https://www.dol.gov/apprenticeship/industry/energy.htm

Veterans who have served and protected the Nation are well-positioned to transition into much needed cybersecurity jobs. Veteran job seekers are more likely than non-veterans to be underemployed, despite the fact that the majority of employers report that they perform "better than" or "much better than" non-veterans. CyberVirginia has launched a Cyber Veterans Initiative that aims to provide training programs, apprenticeships, and employment to veterans of all skill levels, ensuring the programs are accessible in terms of cost and time. Pursuing a similar veterans initiative here in Indiana can similarly dovetail with the critical need for IT/OT professionals, and ensure Indiana is seen as a forward-thinking, economically productive state for a variety of cyber careers.

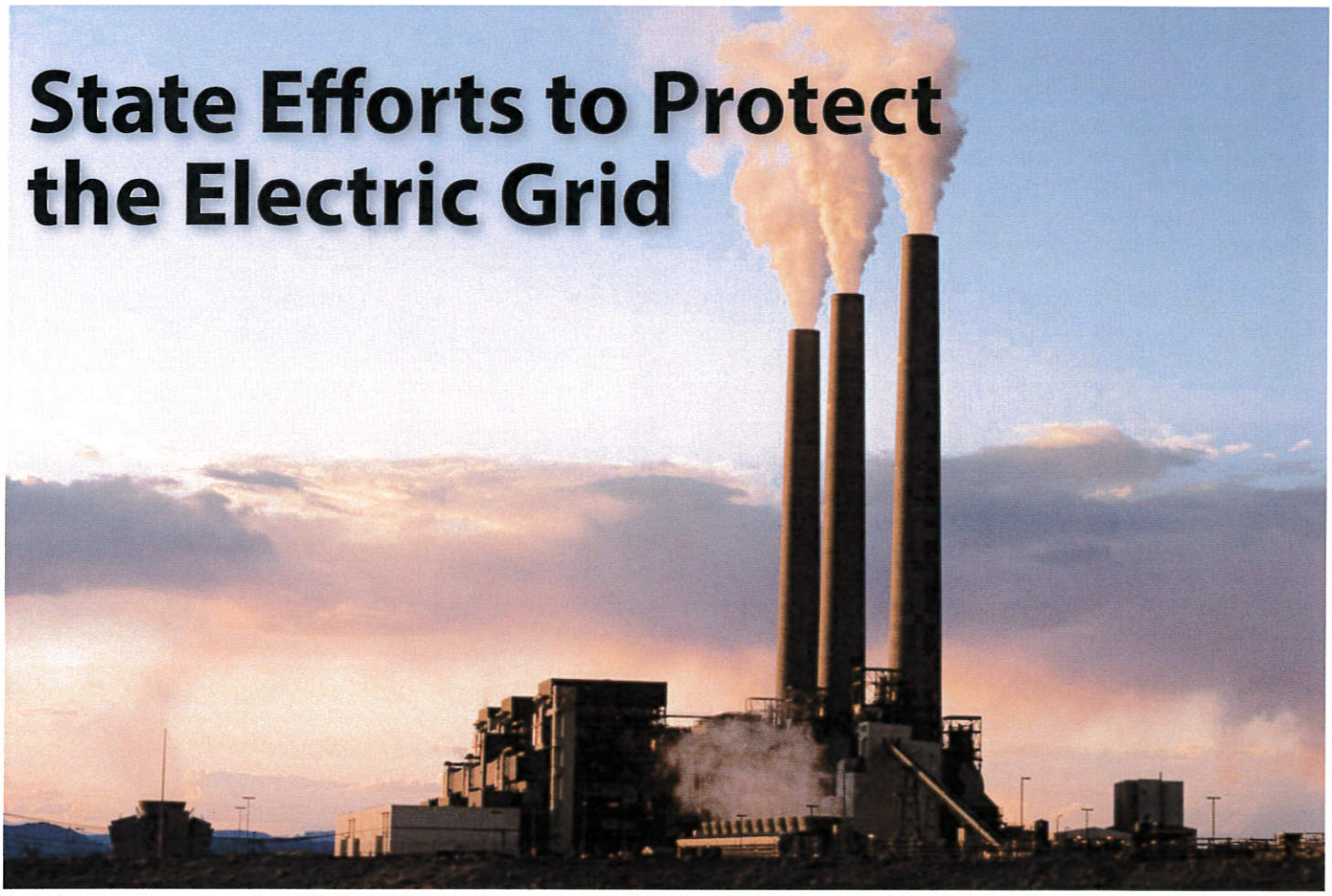
National Conference of State Legislatures (NCSL)

State Efforts to Protect the Electric Grid

April 2016

NCSL
Strong States, Strong Nation

State Efforts to Protect the Electric Grid



BY DANIEL SHEA

April 2016

Overview

There are growing threats to the nation's critical infrastructure and state legislatures have been working diligently to address these issues through a variety of measures. Recent events have highlighted weaknesses in the nation's aging electrical grid, sections of which originated more than a century ago.[1] Even as Superstorm Sandy and Hurricane Irene continue to loom large in the collective memory, Hurricane Joaquin ushered in October 2015 by battering the Eastern seaboard with record levels of rain and 100-mph winds. The increased intensity of recent weather events is raising awareness about the physical threats to the grid. At the same time, a growing array of cyberthreats to energy infrastructure have led experts to increasingly draw attention to the grid's technological vulnerabilities.

Some legislators have sought to make the grid more resilient by diversifying energy production. More than a dozen states introduced legislation in 2015 that calls for greater diversity in power sources—from expanding renewables to supporting nuclear and fossil fuels. At the same time, there has been a significant push to encourage and incorporate microgrids into the electrical system. These standalone systems can operate independently and supply power to a specific area in the event of a broader disruption to the electric system. Some lawmakers are eager to promote microgrids, given the economic impacts of widespread power outages. It has been estimated that a single day without power in New York City would cost $1 billion.[2]

Many states are also considering legislation in support of smart grid technology to not only increase energy system resilience, but also improve reliability and efficiency. These policies can increase the reliability of the electrical grid by improving the management of electricity demand and by

allowing utilities to locate and address failing equipment or power outages more quickly. This technology comes with drawbacks, however, as it opens a door to cyberthreats.

As with many aspects of life, the electrical grid is increasingly interconnected. Millions of new intelligent components are operating in conjunction with legacy equipment that was not designed with modern cybersecurity in mind. These modernization efforts are changing the dynamics of the grid, connecting customer-based smart grid devices and utility control systems to the Internet. While this increased connectivity leads to improved efficiency and grid performance, it also increases the vulnerability to cyberattacks.

The scope of this threat has increased substantially in recent years—with persistent and documented cyber-intrusions into the power grid's critical infrastructure and control systems—leaving some experts to warn that the U.S. power sector is underprepared.[3]

Given that smart grid technologies are considered integral to establishing a 21st century grid, most of the cybersecurity legislation proposed in 2015 revolved around the creation of cybersecurity task forces or committees to study the issue and make recommendations on how to minimize these threats. All of this comes as concerns linger about the physical security of the nation's energy supply. At least 15 bills were introduced in 2015 that address the threat of electromagnetic pulse (EMP) attacks, and at least five bills exempt critical information about the grid and public utilities from disclosure under the Freedom of Information Act.

In all, more than 200 bills relating to energy security and resiliency were introduced in statehouses across the United States in 2015. These state policies play an important role in hardening infrastructure and preparing for disaster response in the event of disruptions and emergencies.

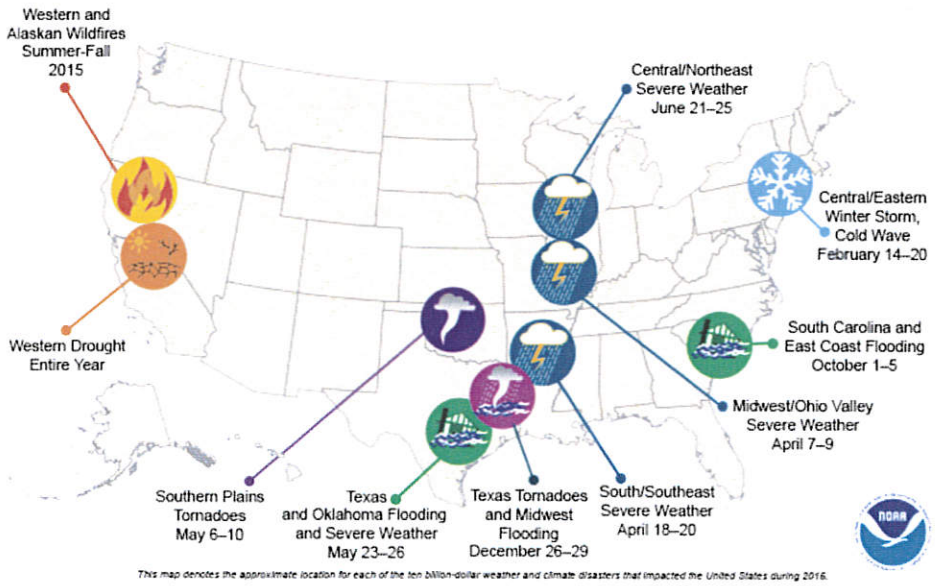
Disaster Preparedness

States have taken a number of steps to ensure that lights will stay on and water will continue to flow in the event of an emergency. These range from requiring standby generators at certain critical facilities to making it easier for out-of-state workers to help with disaster response.

Concerns are growing over the frequency and intensity of natural catastrophes. Data from the U.S. Department of Energy (DOE) shows that weather-related blackouts in the United States doubled between 2003 and 2012. In that same period, 679 widespread power outages occurred due to severe weather, at an annual cost of between $18 billion and $33 billion (Figure 1), according to a report issued by the Department of Energy.[4]

The Atlantic seaboard—where the U.S. Geological Survey says sea-level rise is occurring at rates three-times faster than the global average—is considered especially vulnerable. Two recent reports have compiled information on a number of coastal metropolitan regions, and assessed the vulnerabilities to energy infrastructure by combining factors of sea-level rise and storm surge. The report from the DOE Office of Electricity Delivery and Energy Reliability[5] found that infrastructure in certain regions—such as New York City, Houston and Miami—have a heightened level of risk. New York City alone has around 50 substations and 33 power plants that currently are located in areas that could be affected by rising seas and storms. A similar report by the Union of Concerned

Figure 1. U.S. 2015 Billion-Dollar Weather and Climate Disasters



This map denotes the approximate location for each of the ten billion-dollar weather and climate disasters that impacted the United States during 2015.

Scientists[6] found that more than 400 major substations and nearly 70 power plants currently are exposed to flooding from hurricanes and storm surge in five metropolitan regions.

This trend is expected to continue and even increase in the coming decades. A flurry of recent studies have explored this issue and found that major storms are expected to occur more frequently,[7] and that the resultant flooding will be more severe by the close of the century.[8] A report commissioned by the Massachusetts Senate[9] warned that the state's infrastructure—including 12 power plants and LNG storage facilities located on land less than 10 feet below high tide—will face growing risks of flooding if steps are not taken quickly.

Nearly 40 percent of the U.S. population—over 123 million people—live in coastal shoreline counties, according to U.S. Census Bureau data.[10] Officials across the political spectrum in these communities are working to address the threat posed by rising seas and other concerns that could affect the electric grid. However, far from being a strictly coastal issue, nearly 20 cities across the United States—including Dallas, New Orleans, San Francisco, Norfolk and Pittsburgh—have hired a "chief resilience officer," whose role is to develop and lead a comprehensive resilience strategy.

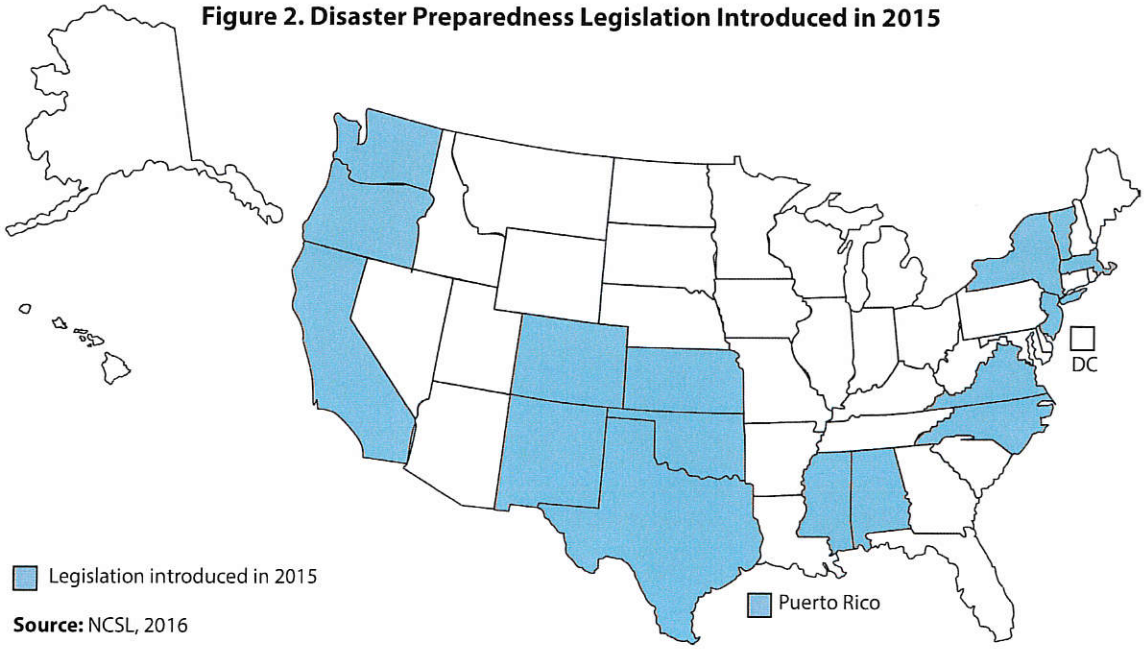
Lawmakers in 16 states and Puerto Rico introduced at least 29 bills to address disaster preparedness in 2015 (Figure 2), while 22 bills were introduced in 2014. Seven states—Alabama, Kansas, Mississippi, New Mexico, Oregon, Vermont and Virginia—introduced at least 12 bills that would exempt out-of-state workers and businesses from certain tax and registration requirements when they are responding to disasters.

At least 15 bills encouraged backup power generation, either by requiring that certain critical infrastructure or public shelters maintain backup generators or by offering incentives to residents who invest in energy-generating technologies. Two states—Oklahoma and Texas—proposed bills that would make it illegal for a homeowners' association to prohibit standby generators. At least four bills were intended to ensure access to motor and heating fuels in the event of an emergency. At least six bills relate to creating state response plans, and instruct state agencies to assess the grid's vulnerabilities and make recommendations.

Key bills from 2015

- **California** A.B. 184—(failed-adjourned) would provide energy efficiency and disaster preparedness guidance and assistance for small businesses.
- **Massachusetts**—Four bills (all pending) would establish a comprehensive adaptation management plan in response to climate change.

Figure 2. Disaster Preparedness Legislation Introduced in 2015



Source: NCSL, 2016

- **New Jersey**—A.B. 2579 (vetoed) would authorize municipalities to facilitate private financing of water conservation, energy improvements, storm shelter construction, and flood and hurricane resistance projects. Four bills (all pending) deal with backup generators and on-site generation for critical facilities. A.B. 2586 (vetoed) would establish a commission to study and make recommendations for improving the state's electric utility infrastructure.
- **New York**—A.B. 3007 (enacted) requires an energy audit and disaster preparedness review of residential health care facilities. A.B. 8390 and S.B. 5271 (both pending) would require the state, its political subdivisions, utilities and health care facilities improve preparedness and response and would require critical infrastructure to be protected.
- **North Carolina**—S.B. 436 (failed-adjourned) would direct the utilities commission to perform an assessment on the extent to which the state's electrical grid is prepared for an emergency.
- **Vermont**—H.B. 320 (enacted) establishes a petroleum set-aside system for liquid fossil fuels to be used in times of emergency or shortages.
- **Puerto Rico**—H.R. 108 (enacted) orders a comprehensive study of infrastructure, including systems for electricity, water and sewage, and other matters relating to security during a public disaster.

Key bills from 2014

- **New Jersey**—Five bills (all failed-adjourned) would require or offer incentives for installation of emergency generators at certain dwellings and facilities. Three bills (all failed-adjourned) would require public utilities to file emergency response and flood mitigation plans. Two bills (both failed-adjourned) would address the issue of motor fuel availability during emergencies. A.B. 1199 (failed-adjourned) would require electric distribution lines to be located underground in areas that are affected by severe weather or natural disasters.
- **New York**—A.B. 8387 (failed-adjourned) would direct several cities to conduct studies on the preparedness and readiness to respond to certain disasters.

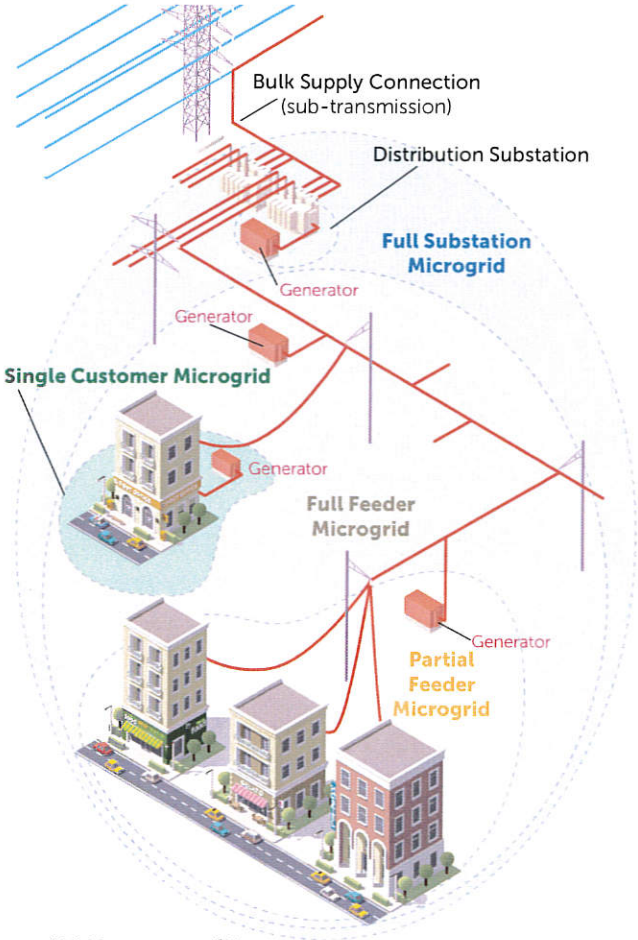
Microgrids

Legislators in at least 17 states introduced bills in 2015 that promote microgrids, often noting that these systems can serve an important role in an emergency. Microgrids can be designed in various ways and can include a variety of resources—utilizing everything from renewables to diesel generators—but they all provide independent power generation to a specific geographic area. The key resiliency component is the microgrid's ability to operate independently from the larger grid (Figure 3).

So, when a major power outage occurs, as happened in the aftermath of Superstorm Sandy, a microgrid can supply homes and businesses with electricity. In fact, while Superstorm Sandy knocked out power for 8.7 million customers across 24 states, a microgrid known as "Co-op City" in the Bronx was able to provide heat, electricity and hot water for 60,000 residents. Similarly, Princeton University and New York University were able to supply heat and power to parts of their campuses throughout the storm.

Figure 3. How a Microgrid Works

A system with its own power resources, loads and definable boundaries that can operate independently or in conjunction with the area's main electrical grid.



Source: U.S. Department of Energy

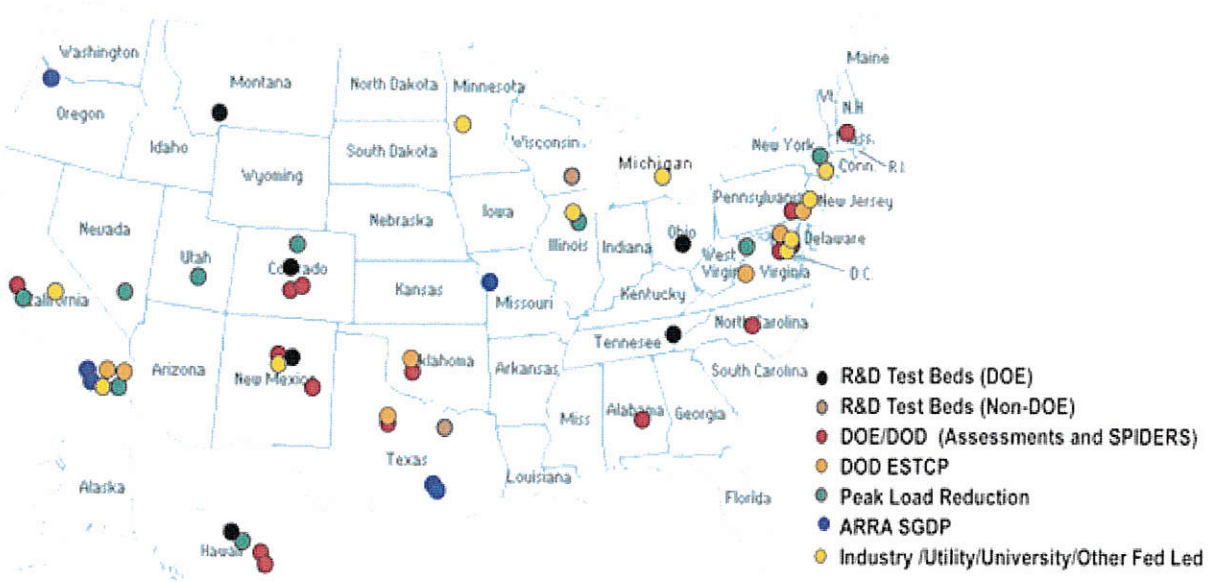
The East Coast is not the only area where microgrids are gaining ground. There are several federal initiatives through the DOE that support microgrid development across the United States (Figure 4). At the state level, bills emerged in a number of states that face hurricanes, earthquakes, tornados, winter storms and other threats. In the West, wildfires have been a regular cause of power outages in recent years, and some California tribes have developed microgrids that expand access to electricity in rural areas and help prepare for emergencies. On several occasions, a Miwuk Indian-owned microgrid has proven its ability to supply its own power for up to 10 days without grid access during wildfires.

While much of the discussion about microgrids has centered on their use in disaster scenarios, some lawmakers have also noted their ability to help diversify sources of energy generation. At least 28 bills were introduced in 2015. At least 11 bills in six states—Alaska, Connecticut, Colorado, Massachusetts, Maryland and New Jersey—offered grants, loans or other incentives to encourage the development of microgrids or similar structures.

Key bills from 2015

- **California**—A.B. 1530 (pending) would promote deployment of clean distributed energy and prioritizes deployment of smart grids and microgrids.
- **Connecticut**—H.B. 6991 (enacted) authorizes the Connecticut Green Bank to help finance energy improvements, including clean energy resources used in the creation of a microgrid, along with any related infrastructure.
- **Hawaii**—H.B. 264 (pending) would require the Public Utilities Commission to establish a process for electricity consumers to form microgrids to provide secure and reliable power when the central grid is down. Three resolutions urged utilities and the Public Utilities Commission to adopt policies that would support microgrids.
- **Illinois**—H.R. 3327 (pending) would require a report and workshops to illustrate how development of microgrids could strengthen the electric grid through reliance on the diverse supply options.

Figure 4. U.S. Department of Energy Microgrid Landscape



- **Maryland**—H.B. 1087 and S.B. 398 (both enacted) establish a pilot program for community solar.
- **Minnesota**—H.B. 3a (enacted) makes changes to energy provisions and requires that utilities issue reports that outline investments considered necessary to modernize and enhance the reliability of the grid, including energy storage and microgrids.
- **New Jersey**—At least eight bills have been introduced over the past two years that require or encourage backup generators. A.B. 4180 and S.B. 2691 (failed-adjourned) would establish microgrid pilot programs to equip critical public facilities with microgrids.
- **New York**—A.B. 6746 (pending) would require the Public Service Commission to develop recommendations for establishing microgrids, including critical buildings and the geographic areas where microgrids should be a priority.
- **Washington**—H.B. 1095 (enacted) requires a life-cycle cost analysis before construction or renovation of critical government facilities to determine the potential for combined heat and power systems that are able to serve public health and safety during a natural disaster or other emergency in which there may be a widespread power outage.

Distributed Generation and Diversification

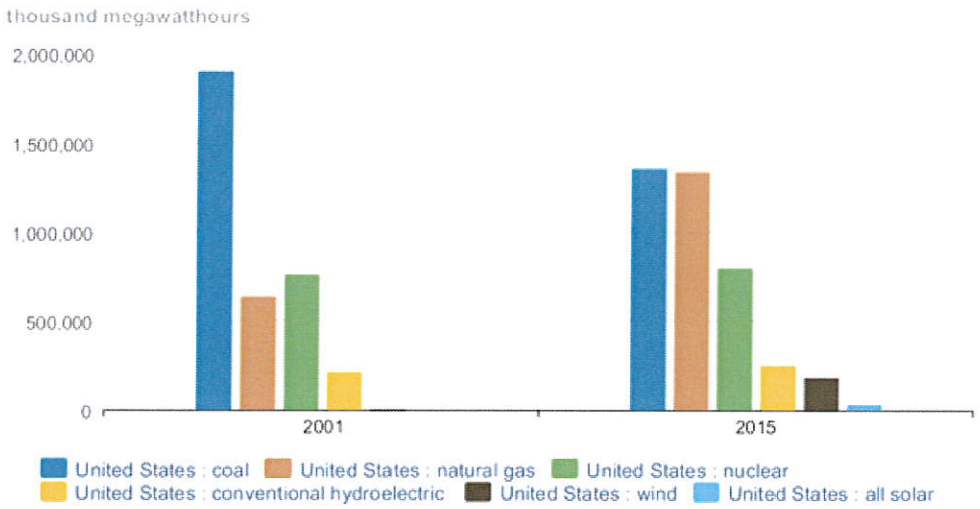
Distributed generation—power generation at the point of consumption—can help keep the lights on during a disaster. In addition, these resources have the potential to lower a utility's peak load, which can improve reliability.[11]

In crafting legislation, however, some lawmakers also used the concept of distributed generation to call for the continued diversification of state energy portfolios (Figure 5). The West Coast—and Hawaii, in particular, where electric rates are higher than in any other state due to dependence on imported fossil fuels for electricity generation—pushed this message by offering incentives to invest in renewables as a means of achieving energy independence. Other states encouraged diversification of the energy supply through coal, natural gas, biomass, offshore wind, nuclear and waste-to-energy.

Key bills from 2015

- **California**—S.B. 350 (enacted) requires an increase in the amount of electricity generated and sold from renewable energy resources in order to strengthen the diversity and resilience of the electrical system.
- **Hawaii**—H.B. 1273 (enacted) authorizes the construction of hydroelectric facilities of not more than

Figure 5. Net Generation for all Sectors, Annual



Data Source: U.S. Energy Information Administration

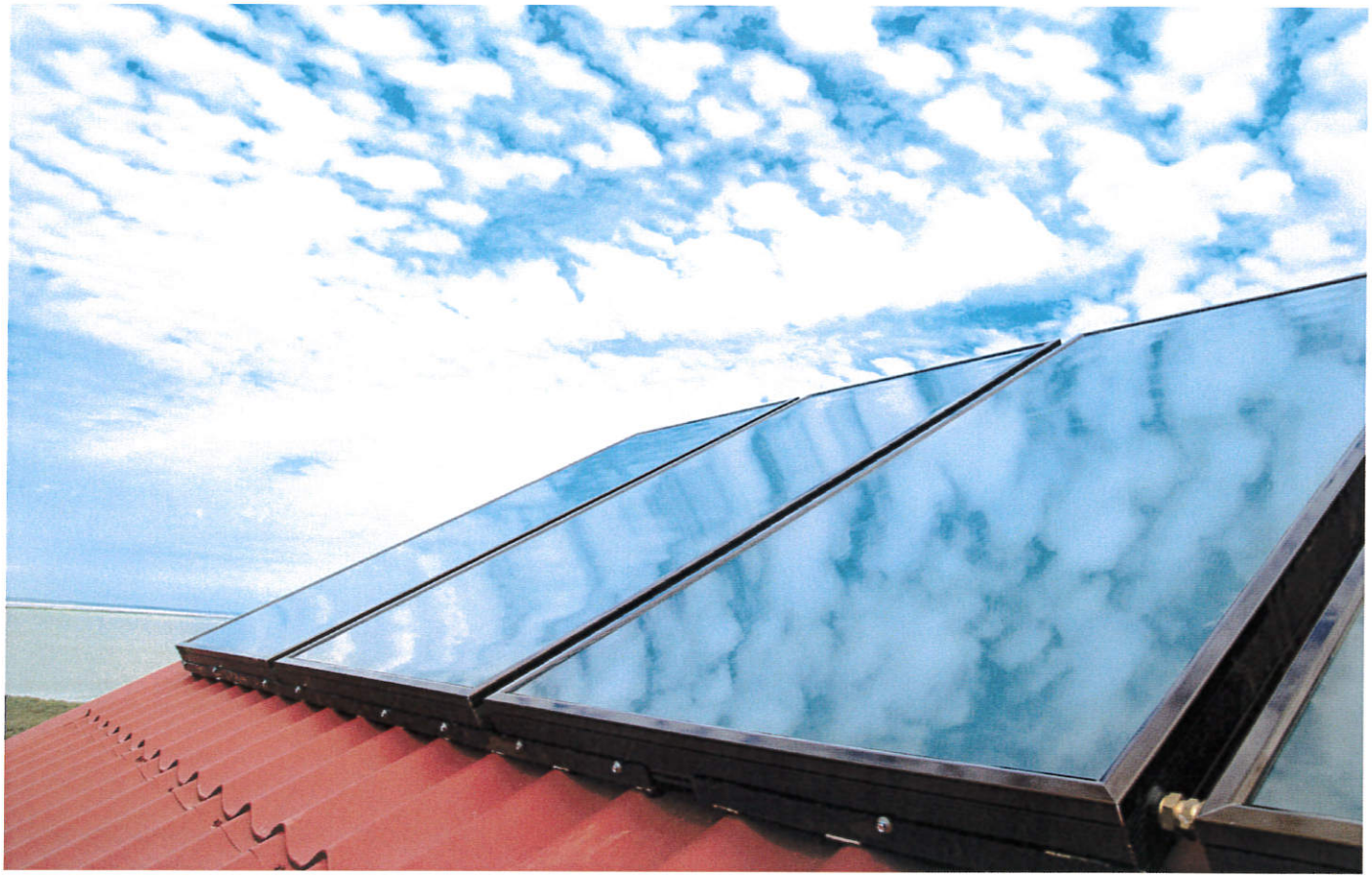
500 kilowatts on agricultural lands. H.B. 1286 (enacted) encourages energy efficiency, renewable energy and a reduction in state dependence on fossil fuels. S.B. 1050 (enacted) allows utility customers to elect to participate in renewable community energy projects. S.B. 1047 (pending) would authorize bonds to help develop a waste-to-energy plant.

- **New York**—A.B. 107 (pending) would require the development of a statewide shared renewable energy zone map and would provide for the interconnection of shared solar, farm waste, micro-combined heat and power, fuel cell, micro-hydroelectric and wind generation.
- **Ohio**—H.C.R. 9 (enacted) establishes a sustainable energy abundance plan to meet future energy needs, including new nuclear generation technology.
- **Utah**—S.B. 280 (enacted) promotes development of diverse energy resources, including nonrenewable and renewable resources, nuclear and alternative transportation fuels.
- **Vermont**—H.B. 40 (enacted) creates a program for electric utilities, sets certain requirements for renewable energy or renewable energy credits, and encourages distributed generation.
- **Virginia**—S.B. 1349 (enacted) requires that electric utilities file integrated resource plans in order to diversify their generation supply portfolio.
- **Washington**—Three bills—H.B. 1897 (enacted), S.B. 5024 (enacted), and H.B. 1912 (pending)—extend or would extend incentives for renewable energy and encourage or would encourage development of clean energy. S.B. 5113 (pending) would support small modular reactor siting and development.

In addition, at least nine bills sought to study or develop energy storage. Energy storage has been viewed as another form of redundancy in the grid, with the potential to provide backup power in the event of an outage by storing electricity in batteries. Several states also have sought to explore the possibility of vehicle-to-grid technologies, which would allow electric vehicles to supply backup power to the electric grid in the event of an energy shortfall or outage. Another seven bills addressed alternative fuels.

Key bills from 2015

- **California**—Three bills (all pending) would address energy storage and require the Public Utilities Commission to study energy storage and the role that electric vehicles could play. Three bills (all failed) would promote alternative fuels by adopting a renewable gas standard or providing support to in-state production of alternative fuels.
- **Connecticut**—S.B. 1078 (enacted) requires the state to seek proposals that provide for passive demand response, including energy storage solutions. Two other bills addressed energy storage and the role of electric vehicles.
- **Hawaii**—S.B. 349 (vetoed) would have established a renewable fuels production tax credit to encourage local production of renewable fuels.
- **Massachusetts**—H.B. 2852 and S.B. 1770 (both pending) would offer tax exemptions and other promotions to encourage community shared solar systems and energy storage programs.
- **Minnesota**—H.B. 1320 (pending) would establish a rebate plan to encourage purchase of energy storage



systems that can help with load management. H.B. 2081 and S.B. 1948 (both pending) would require public utilities to file plans that promote electric vehicles and would require a pilot program for vehicle-to-grid technology.

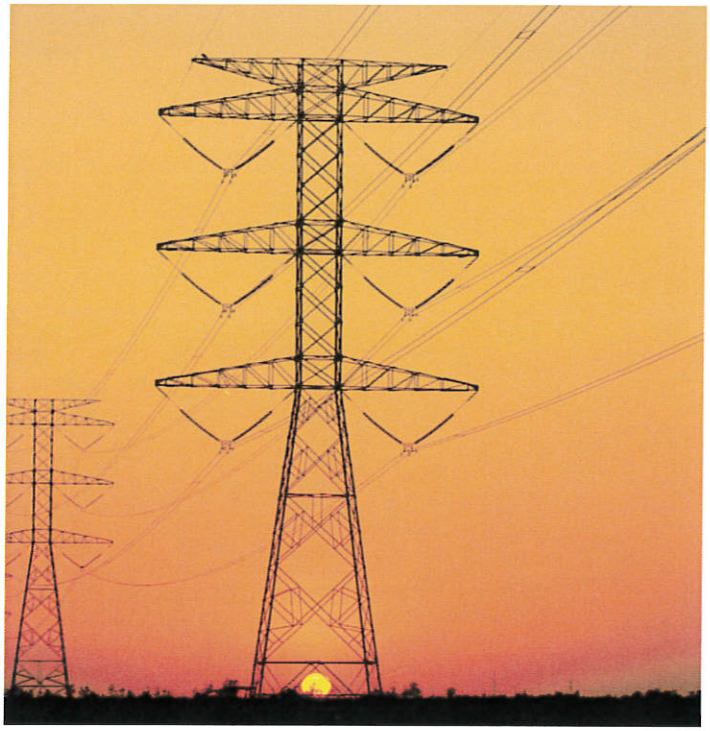
- **Oregon**—H.B. 2193 (enacted) directs electric companies to procure energy storage systems, allowing them to recover all costs through electrical rates.

Comprehensive Plans and Utilities

The electrical grid is undergoing rapid transformations, and states are playing a major role in that development. There is momentum across the country to modernize the grid. This often refers to the promotion of smart grid technologies, which allow customers and utilities to use energy more effectively and efficiently. In 2015, legislators in six states introduced at least 12 bills outlining comprehensive plans to modernize the electrical grid and make it more reliable through a combination of policies that promote energy efficiency, demand-response programs and on-site generation.

Key bills from 2015

- **California**—S.B. 83 (enacted) requires public utilities to enact net metering tariffs to enhance diversification and reliability of the state's energy resources and to encourage private investment in renewable energy and energy efficiency.
- **Illinois**—S.B. 1879 (pending) would establish a renewable energy fund, photovoltaic requirements, voltage optimization, demand-response, net metering, microgrids and low-income programs.
- **Minnesota**—H.B. 3a (enacted) requires that utilities issue reports every other year that describe transmission and distribution plans that outline investments considered necessary to modernize and enhance the reliability of the grid, including improvements to physical and cybersecurity, net metering, control technologies, energy storage, demand-response and microgrids.
- **New Hampshire**—H.B. 362 (enacted) requires each utility to file a resource plan in which it forecasts future demand; assesses energy management and supply options; and assesses distribution and transmission requirements, including benefits and costs of smart grid



technologies and other programs to ensure a more reliable and resilient grid. H.B. 614 (enacted) implements the goals of the 10-Year Energy Strategy, which include grid modernization.

- **New York**—A.B. 2371 (pending) would address aging infrastructure, establish a grid modernization program and create the Smart Grid Advisory Council.
- **Rhode Island**—S.B. 2439 and H.B. 7991 (both enacted) establish a framework for the state to coordinate with other New England states to make strategic investments in resources and infrastructure.

Another 21 bills introduced in 2015 required specific grid updates to improve system reliability. These actions include requiring utilities to file plans for the acquisition of smart grid technologies, requiring public utilities commissions to consider changes to the regulatory structure in light of distributed generation, and authorizing the development of regional organizations to improve reliability and efficiency.

Key bills from 2015

- **California**—A.B. 793 (enacted) requires weatherization and electrical and gas corporations to develop programs for acquisition of certain technology. S.B. 155 (pending) would authorize the independent system operator to enter into a multistate entity that would enhance the reliability and supply of the electrical grid.
- **Colorado**—S.B. 120 (pending) relates to a requirement that each provider of retail electric service in Colorado develop an electric grid modernization plan.
- **Illinois**—H.B. 3975 (enacted) provides for upgrades and modernizes the state's transmission and distribution infrastructure, including smart grid electric system upgrades.
- **Minnesota**—H.B. 2032 (pending) would require a study of the feasibility of creating a state public power authority with the power to construct and operate electric generation and transmission facilities.
- **Virginia**—H.B. 2237 and H.B. 1334 (both enacted) allow utilities to set rate increases to recover the costs of installing solar energy facilities and making improvements to the distribution system.
- **Washington**—H.B. 1895 (pending) would require electrical companies to file a smart grid technology report.

Cybersecurity

Since the U.S. Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT) began publishing reports in 2011, the energy sector has been the most targeted sub-sector of all U.S. critical infrastructure.[12] The energy sector has gone from being the target of nearly 60 percent of reported incidents in 2013 down to 16 percent in 2015,[13] when attackers turned their attention to industrial control system vendors.[14] A successful attack on a vendor could compromise vendor devices and provide access to power sector industrial control systems that regulate power management. This exemplifies how cyberthreats are evolving, requiring diligent surveillance and constant adaptation. More than half of all reported incidents were advanced persistent threats or sophisticated actors, according to ICS-CERT.

The nation's energy infrastructure faces a new range of threats as grid modernization efforts bridge the gap between two very different generations of technologies. "New components will operate in conjunction with legacy equipment that may be several decades old, and provide little to no cyber security controls," according to a report from the Electric Power Research Institute (EPRI).[15] In addition, information technology and operations technology have converged, linking computer systems with physical, equipment-oriented technology.

Concerns exist about what this means for the U.S. grid. Several high-profile incidents have proven that malware and other cyberthreats can result in physical damage to equipment and even service disruptions. However, most of these examples have occurred in areas of the world without the same level of cyberdefenses which have been deployed in the United States. In fact, an ICS-CERT 2015 report notes that, while there continue to be a number of incidents that result from "insufficiently architected networks," there have also been signs of significant improvement, given that nearly 70 percent of reported incidents had no evidence of successful intrusion by attackers. Attackers were almost 20 percent more successful at intruding networks in 2014.[16]

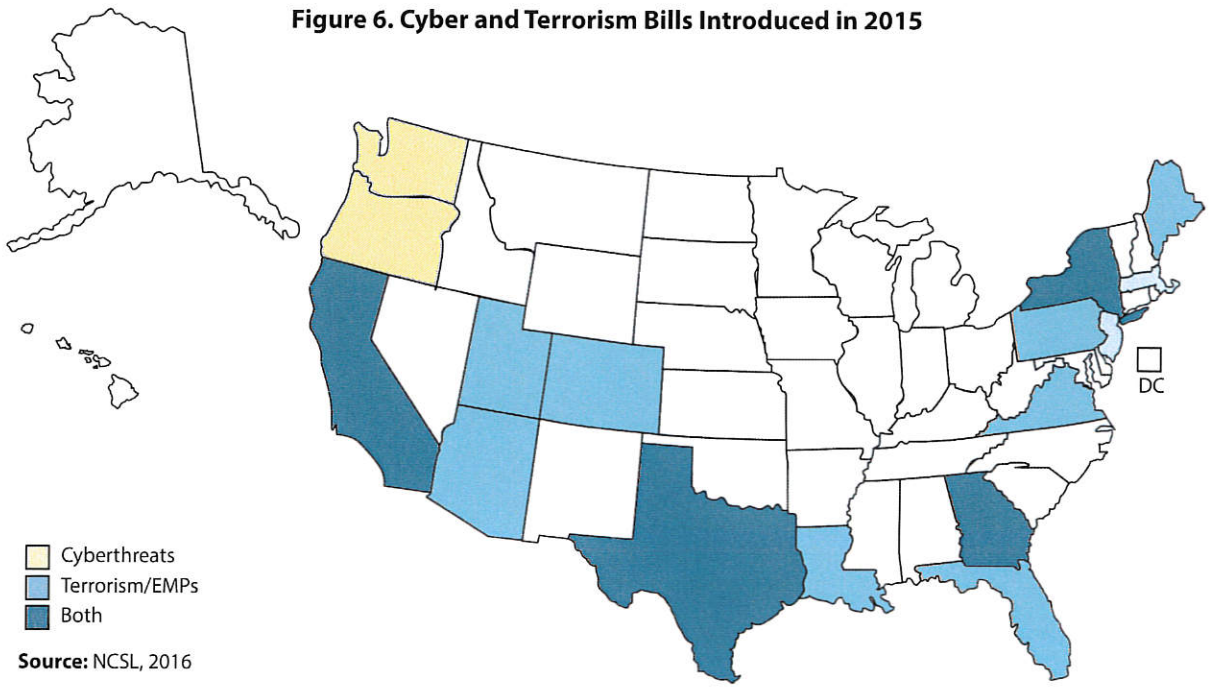
Supervisory control and data acquisition (SCADA) systems are one type of industrial control which are of particular concern. SCADA systems, in use since the 1970s, allow for the remote control of complex system operations over a wide territory. However, these systems were not designed with the Internet—let alone cybersecurity—in mind, and there have been documented incidents in which SCADA systems have been compromised through malware.

It will be decades before legacy equipment is phased out. In the meantime, EPRI suggests that systems be designed and implemented with cybersecurity as a primary concern.[17] "Cyber security must be included in all phases of the system development life cycle, from the design phase through implementation, operations and maintenance," according to another EPRI report.

To address these vulnerabilities, the electric power industry has been coordinating with the North American Electric Reliability Corporation (NERC) and federal agencies such as the National Security Agency (NSA), the Federal Energy Regulatory Commission (FERC), the U.S. Department of Homeland Security and the U.S. Department of Energy. FERC has approved new cybersecurity standards developed by NERC that aim to enhance the grid's protections. These updated standards—Critical Infrastructure Protection Version 5 (CIP V5)—are considered more robust and proactive. Previous versions applied only to utilities of a certain size, but CIP V5 affects the grid at all levels.

Although the federal government plays a significant role in countering these threats, utilities and states are also taking steps to strengthen cyberdefenses. Not only do states participate in NERC-sponsored grid security exercises like GridEx, but many also are exploring ways to address grid vulnerabilities and ensure that state response agencies are prepared. At least 16 bills or resolutions sought to address the issue at the state level in 2015 (Figure 6).

Figure 6. Cyber and Terrorism Bills Introduced in 2015



Source: NCSL, 2016

Key bills from 2015

- **California**—A.B. 853 (pending) would require that utilities use their own employees for work involving computer and other critical systems of nuclear, electrical and gas infrastructure in order to protect the integrity and security of the state's critical infrastructure. A.B. 1172 and A.B. 2200 (both pending) would require the state's Cyber Security Task Force to meet quarterly, and would create the Cyber Security Steering Committee within the governor's Office of Emergency Services.
- **Georgia**—Five bills (all pending) would create committees to address cybersecurity.
- **New York**—A.B. 6130 and S.B. 3407 (both pending) would require formation of a cybersecurity advisory board. A.B. 6133 and S.B. 3405 (both pending) would require a comprehensive review of all cybersecurity services to be performed every five years.
- **Oregon**—H.B. 3394 (pending) would establish a cybersecurity task force.
- **Washington**—H.B. 1468 (pending) would grant the governor authority to proclaim a state of emergency in the event of a cybersecurity incident. H.B. 1470 (pending) would establish a blue-ribbon panel on cybersecurity.

Terrorism

Physical threats to the power grid and other critical infrastructure also concern many lawmakers. At least 15 bills were introduced in 2015—and another four the previous year—aimed at protecting the electrical system against an electromagnetic pulse (EMP) attack. Of these, five states—Colorado, Georgia, New Jersey, New York and Texas—considered legislation that would have created committees to study the vulnerabilities and effects of an EMP attack and to evaluate technologies to address those issues. Meanwhile, three states—Florida, Pennsylvania and Texas—urged federal action to harden the grid against such attacks.

At the same time, at least five bills were introduced that exempted certain detailed information about the grid, utilities and state energy infrastructure from disclosure under the Freedom of Information Act. Four of these bills passed—in Arkansas, California, Kansas and Virginia.

Key bills from 2015

- **Massachusetts**—H.B. 3526 (pending) would require electric companies to develop and implement plans to address the vulnerabilities of the electrical grid to natural and EMPs and other manmade and natural occurrences.
- **New York**—A.B. 6657 and S.B. 2385 (both pending) would empower the state to decide if the sale, lease or operation of any critical infrastructure owned by the state would threaten public security, and creates the Critical Infrastructure Advisory Council.
- **Virginia**—S.B. 1238 (enacted) requires the state Department of Emergency Management to specifically plan for disasters caused by EMPs and geomagnetic disturbances.
- **Utah**—H.J.R. 26 (enacted) requires a study of the steps Utah has taken to protect its electrical grid and to examine work done in other states.

Key bills from 2014

- **Arizona**—S.B. 1476 (enacted) requires the state Department of Emergency and Military Affairs to develop preparedness recommendations in the event of an EMP.
- **Louisiana**—S.R. 169 (adopted) requests the governor's Office of Homeland Security and Emergency Preparedness to study the potential threats and consequences of an EMP.
- **Virginia**—S.J.R. 61 (enacted) directs the Joint Commission on Technology and Science to study the nature and magnitude of potential threats caused by geomagnetic disturbances and EMPs and to recommend strategies to protect infrastructure.

Funding

Lawmakers in five states introduced at least 10 bills to help fund improvements to the state electrical grid that would enhance energy security, reliability and resiliency. Hawaii introduced five of these bills, three of which have been enacted.

Key bills from 2015

- **Hawaii**—H.B. 1513 (enacted) establishes a two-year matching grant pilot program to strengthen local

companies that are conducting renewable energy research and development in order to reduce the state's dependence on fossil fuels. S.B. 359 (enacted) requires that 15 cents of the tax on each barrel of petroleum be deposited into the Energy Security Special Fund, and that 10 cents on every barrel be deposited into the Energy Systems Development Special Fund. S.B. 892 (enacted) appropriates money for resilience and sustainability strategy, including $25 million to improve efficiency, grid operations and resiliency.

- **New York**—A.B. 5883 (pending) would establish the New York State Infrastructure Development Bank, and would appropriate $250 million to support infrastructure improvement projects.
- **Washington**—H.B. 115 (enacted) allocates funds, including $28 million for grants to advance clean energy and enhanced transmission and distribution control systems, and for utility projects that demonstrate smart grid technologies.

Notes

1. American Society of Civil Engineers, *2013 Report Card for America's Infrastructure 2013* (Reston, Va.: ASCE, March 2013), http://www.infrastructurereportcard.org/energy.
2. Arup, Regional Plan Association (RPA) and Siemens, *Toolkit for Resilient Cities: Case Study: New York City Electrical Grid (n.p.: Siemens, 2013),* http://w3.siemens.com/topics/global/en/sustainable-cities/resilience/Documents/pdf/Toolkit_for_Resilient%20Cities_NY_Case_Study.pdf.
3. Richard J. Campbell, *Cybersecurity Issues for the Bulk Power System* (Washington, D.C.: Congressional Research Service, June 10, 2015), https://www.fas.org/sgp/crs/misc/R43989.pdf.
4. U.S. Department of Energy, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages* (Washington, D.C.: U.S. DOE, August 2013), http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
5. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, *Sea Level Rise and Storm Surge Effects on Energy Assets* (Washington, D.C.: U.S. DOE, n.d.), http://icfgeospatial.maps.arcgis.com/apps/MapSeries/index.html?appid=58f90c5a5b5f4f94aaff93211c45e4ec.
6. Union of Concerned Scientists, *Lights Out? Storm Surge, Blackouts, and How Clean Energy Can Help* (Cambridge, Mass.: Union of Concerned Scientists, 2015).
7. Anita J. Reed et al., "Increased threat of tropical cyclones and coastal flooding to New York City during the anthropogenic era," *Proceedings of the National Academy of Sciences* 112, no. 41 (Oct. 13, 2015).
8. Christopher M. Little et al., "Joint projections of US East Coast sea level and storm surge," *Nature Climate Change* 5 (Sept. 21, 2015): 1114-1120.
9. Commonwealth of Massachusetts, Report of the Senate Committee on Global Warming and Climate Change, *No Time to Waste* (Boston: Massachusetts General Court, Feb. 13, 2015), http://archives.lib.state.ma.us/handle/2452/264298.
10. National Oceanic and Atmospheric Administration, *NOAA's State of the Coast* (Washington, D.C.: NOAA, 2010), http://stateofthecoast.noaa.gov/.
11. U.S. Department of Energy, *The Potential Benefits of Distributed Generation and Rate-Related Issues That May Impede Their Expansion* (Washington, D.C.: U.S. DOE, February 2007), https://www.ferc.gov/legal/fed-sta/exp-study.pdf.
12. U.S. Department of Homeland Security, "Industrial Control System Cyber Emergency Response Team (ICS-CERT)," *ICS-CERT Monitor* (September 2014-February 2015), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.
13. U.S. Department of Homeland Security, ICS-CERT, "Notable Incident," *ICS-CERT Monitor* (November-December 2015), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT%20Monitor_Nov-Dec2015_S508C.pdf.
14. U.S. Department of Homeland Security, ICS-CERT, "Trends in Incident Response in 2013, *ICS-CERT Monitor* (November-December 2013), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf.
15. Electric Power Research Institute (EPRI), *Risk Management in Practice: A Guide for the Electric Sector* (Palo Alto, Calif.: EPRI, Dec. 15, 2015), http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002003333.
16. U.S. Department of Homeland Security, ICS-CERT, "Notable Incident."
17. EPRI, *Cyber Security Strategy Guidance for the Electric Sector* (Palo Alto, Calif.: EPRI, May 30, 2012), http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001025672.

NATIONAL CONFERENCE *of* STATE LEGISLATURES

William T. Pound, Executive Director

7700 East First Place, Denver, Colorado 80230, 303-364-7700 | 444 North Capitol Street, N.W., Suite 515, Washington, D.C. 20001, 202-624-5400

www.ncsl.org

ISBN 978-1-58024-851-8