AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

# Cybersecurity Program Update

www.PublicPower.org/GridSecurity

# Improving Grid Security in Public Power

In June 2016, the American Public Power Association entered into Cooperative Agreement #DE-OE0000811 with the U.S. Department of Energy for a three-year program, with total funding of $7.5 million, to improve the cyber and physical security posture of public power utilities.

In the first year of the program, the Association conducted activities in five areas:

1. Cyber resiliency and security assessments
2. Onsite vulnerability assessments
3. Security training and resource development
4. Deployment of security technologies
5. Implementation of information sharing mechanisms

The Association thanks the more than 150 public power utilities that participated in the program (see list in Appendix A) during year 1 for sharing their expertise.

This update summarizes the Association's accomplishments in year 1, discusses activities for years 2 and 3, and outlines program benefits to public power utilities.

# Cyber Resiliency and Security Assessments

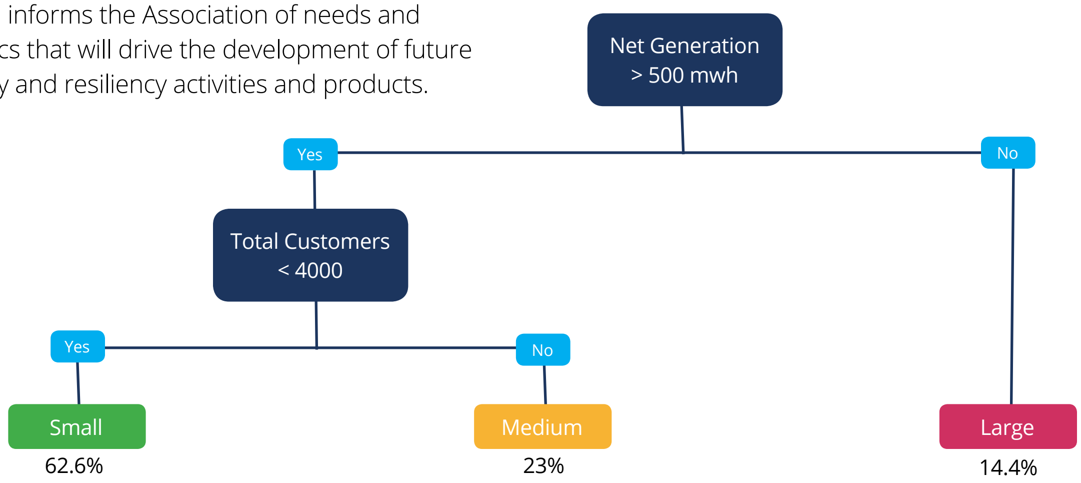
## Research and Analysis

To assess the cyber maturity of public power utilities, the Association conducted research to define member demographics and general security capabilities and resiliency. The research results and analysis are captured in the Public Power Baseline Assessment. Criteria were established to categorize small, medium, and large public power utilities for the cybersecurity work.

The baseline informs the Association of needs and demographics that will drive the development of future cybersecurity and resiliency activities and products.

## NEXT STEPS

The Association will conduct additional assessments of the security capabilities and needs of small and medium sized public power utilities.



| Cluster | Utilities | Customer Count | NERC Registered Entities |
|---|---|---|---|
| **Large** | **290** | **0 to 1,458,330; Avg. = 49,575** | **157** |
| **Medium** | **461** | **4,015 to 408,411; Avg. = 15,156** | **88** |
| **Small** | **1255** | **0 to 3,995; Avg. = 1,314** | **14** |

**Figure 1: Demographics of public power utilities.**
Source: Axio Global, Inc.

Note: North American Electric Reliability Corporation registered entities were assumed to have an existing cyber program in place and were not included in this initial assessment.

## Public Power Maturity Model: Cybersecurity Scorecard

During the assessment phase of the program, a quick launch self-assessment tool — the Public Power Cybersecurity Scorecard — was created. The scorecard was modeled after the U.S. Department of Energy's electricity subsector Cybersecurity Capability Maturity Model, or C2M2.

The scorecard is designed for small and medium public power utilities that are just starting to evaluate their cybersecurity program. A self-assessment gives a utility the starting point to address cyber risks and informs utility leadership on cyber risk decisions.

In year 1, the scorecard was tested in a user group, which provided feedback. The scorecard will be further tested in year 2 and be made available online.

The scorecard comprises 14 questions which a utility can answer in 45 minutes — compared to the two-day facilitated session needed to complete the C2M2 model. Answers to the scorecard questions can be incorporated into the C2M2 when a utility is ready to use the model.

The 14 questions in the scorecard address these key areas:

- Cyber asset inventory
- Configuration baseline
- Access control
- Vulnerability management
- Threat management
- Cyber risk management
- Cyber event detection
- Cyber incident response
- Operational resiliency
- Monitoring cyber system activity
- Cyber threat and event information sharing
- Supply chain risk
- Workforce management and cyber security training
- Cybersecurity program management

The scorecard gives public power utilities the ability to determine their general cybersecurity posture without extended time and cost commitments.

### NEXT STEPS

The Association will encourage its members to use the scorecard to conduct self-assessments of their cybersecurity posture and will undertake further cybersecurity and resiliency activities, including

- Make the scorecard available online
- Obtain an adequate sample size for each utility category to improve benchmarking
- Update the baseline to reflect scorecard responses
- Target categories for cybersecurity program resources and training, based on scores shared voluntarily
- Create profiles for a public power utility based on its demographic cluster and identification of trends for each group
- Incorporate the scorecard answers to the C2M2 and provide a target profile recommendation for a mature cybersecurity program

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

# Security Vulnerability Onsite Assessments

During year 1 of the program, the Association conducted 11 in-depth onsite vulnerability assessments and provided detailed security improvement reports to each utility that participated. Common cybersecurity challenges were identified, such as limited documentation of cybersecurity incident history and the physical security of cyber assets, limited cybersecurity staff, and limited cybersecurity policies and procedures. These challenges will be the focus of the Association's security training and resource development in years 2 and 3 of the program.

It is recommended that public power utilities conduct onsite assessments to receive specific recommendations on enhancements to improve its cybersecurity readiness.

## NEXT STEPS

In year 2, the Association plans to conduct 11 additional onsite vulnerability assessments.

The Association will also assess and develop the following:

- Logging and monitoring activities, especially where utilities integrate their information technology (IT) and operations technology (OT) logs
- Simplified assessments on the key areas identified in the scorecard
- Action plans with top priorities highlighted
- Trend analysis to inform future resource development

# Security Training and Resource Development

## Security Training

In year 1, the Association conducted five 2-day, in-person C2M2 facilitated workshops in various regions of the country. In all, the workshops included 124 participants from 41 public power utilities. The workshops trained participants on how to use the C2M2, understand the characteristics of a mature cyber and physical resiliency program, and benchmark the utility's maturity level.

The Association also conducted 14 tabletop exercises for utility executives as well as IT and OT administrators. These exercises focused on sharing threat information and identified some challenges that will be addressed in year 2 of the program.

Cybersecurity classes were held for executives and IT/OT professionals. The classes were developed by three cybersecurity expert trainers.

For executives, the training sessions discussed tools needed to understand the subject matter and help develop the capability to work with internal and external audiences. For IT/OT personnel, the training sessions discussed a particular security domain and provided background theory as well as tools to design and implement a comprehensive cybersecurity program.

The training is intended to elevate executives' understanding of cybersecurity issues so that they can make decisions on security investment and operational needs, and ensure that IT/OT staff are informed about the latest security tools.

During the year 1 training sessions, many public power utilities acknowledged that they would benefit from additional training on identifying cyber risks and developing a cybersecurity program in their organizations.

### NEXT STEPS

The Association will explore and develop low-cost training activities including

- Tabletop exercises — focused on major areas identified in the scorecard — at Association and joint action agency meetings
- Cybersecurity awareness, risk assessments, program and policy development, incident response, information sharing, OT environment cybersecurity, and template development
- Strategies to develop the future cybersecurity workforce
- A public power cybersecurity training certification program
- A Cyber Resilience and Security Incident Playbook, addressing roles and responsibilities in case of a security incident
- A public power cybersecurity summit

## Resource Development

During the year 1 workshops and tabletop exercises, public power utilities identified the need for various cybersecurity resources. The Association developed these resources to help public power utilities build their cybersecurity programs.

**Managed Cybersecurity Service Provider Catalog:** The Association evaluated 48 security services and technology providers to ascertain who can best serve public power utilities and developed the Managed Cybersecurity Service Providers Catalog. Utilities can review the products and services — including subscription services — available to address cybersecurity needs.

The Association does not endorse any of the products or services in the catalog. But utilities can use it to:

- Determine and prioritize their cybersecurity needs
- Review vendor profiles and offerings and obtain contact information
- Discuss offerings with providers and determine if the level of security provided is above, below, or level with requirements

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

# Security Training and Resource Development

- Gauge the costs of outsourcing cybersecurity to these companies by asking for detailed quotes, including installation fees and recurring costs
- Select providers based on needs and assessments

**Videos:** Several videos were produced in year 1 to provide general awareness to public power utilities on cybersecurity risks and the Association's cybersecurity program. Videos are available on a program overview, cybersecurity 101, and cyber risk assessment.

**Cybersecurity Information Engagement Plan:** The Association developed an engagement plan to be used by public power utilities to inform city officials on cybersecurity issues. The plan will help utilities engage with government officials and other key stakeholders on cyber and physical security issues. One key recommendation of this report is to designate a cybersecurity program lead within the utility to champion a cybersecurity program.

**eReliablity Tracker and ICE Calculator Integration:** The Association offered an 80% discount on 3-year subscriptions to its eReliability tracking service to encourage small public power utilities to leverage this service. The goal was to give the smallest public power utilities the ability to transition from paper reliability records to automated systems.

The Interruption Cost Estimate or ICE Calculator is designed for electric reliability planners at utilities, or other entities that are interested in estimating interruption costs and/or the benefits associated with reliability improvements.

During year 1, the Association developed new algorithms and integrated the ICE Calculator into the eReliability Tracker. Public power utilities can now use their outage history to make cost-based reliability decisions inside the integrated tracker. Utilities can also see how much a cybersecurity attack would cost their customers. This information can be used to educate local government officials, and obtain cybersecurity funding.

With this advanced tool, utilities can increase security awareness, make security investment decisions, and get tools to institute a documented cybersecurity program.

## NEXT STEPS

The Association will develop additional resources, including:

- Resources that address the challenges identified in the scorecard and onsite vulnerability assessments
- Advanced reliability and resiliency reporting algorithms incorporated into the eReliability Tracker and ICE Calculator to create predictive resiliency metrics to assess the potential impact of cyber events
- A cyber asset tracker and management platform with a step-by-step guide on how to identify, track, and maintain utility cyber assets
- Research with National Laboratories and universities on the impact of cyber incidents on reliability, resiliency, and costs to inform cyber technology investments
- The Public Power Cyber Resiliency and Security Roadmap outlining strategy and tactics to develop or enhance a cybersecurity program at a public power utility

# Deployment of Security Technology

The Association learned that most small and medium-sized utilities rely on the services of a Managed Security Service Provider (MSSP) to address cyber risks. Discounted subscriptions — through an 80 percent cost share funded by the program — were offered to the N-Dimension N-Sentinel subscription service, which is popular among public power utilities.

Many utilities found even this discounted subscription rate to be a hurdle. The Association found that working with joint action agencies elicited a better response then soliciting individual utilities. Although this form of engagement takes longer, it encourages more deployments and the formation of a more robust regional community. Joint action agencies have more of a stake in the long-term success of the MSSP service deployments.

New technologies and services advance a utility's cyber readiness and expand capability without adding new personnel. However, the utility must maintain the system and act on the cyber threat notifications.

## NEXT STEPS

The Association will continue to research and deploy new technologies and services that will help address cyber risk for public power utilities, including:

- Contracting with joint action agencies for MSSP subscription services
- Developing best practices for deployment by exploring the correlation between utility characteristics and demographics (size, number of IT staff employed, and governance or decision-making structure), and delays in the deployment process
- Leveraging controlled social media platforms to develop a sense of community and engagement to discuss the MSSP threat information and utility actions

# Implementation of information sharing mechanisms

## Secure Information Sharing Mechanisms

Public power utilities, regardless of size, must have easy access to actionable cyber threat information. The Association analyzed the current model of cyber threat sharing through the Electricity Information Sharing and Analysis Center and found that public power utilities need to distill these threat feeds into actionable information.

To overcome this challenge, the Association evaluated information sharing methodologies and technologies that will improve cyber and physical resiliency and security within public power utilities. As part of this research, the Association worked with joint action agencies to encourage all public power utilities to sign up with the E-ISAC.

The research found that

- Public power utilities with the capability to start gathering security event logs should install a Security Event and Information Management (SEIM) solution. At a minimum, security logs should be correlated across the utility.
- Joint action agencies could serve as a centralized repository for their utilities' security logs through the SEIM tools.
- Joint action agencies can filter threat information from E-ISAC to be more actionable for their member utilities.
- When adopting SEIM solutions, it is critical to require the use of standard threat information sharing protocols such as the Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) protocol to ensure interoperability among key stakeholders.
- MSSPs providing SEIM solutions to public power utilities must be able to integrate with a STIX/TAXII solution to create an end-to-end security event log management and threat information sharing process for the industry.

The Association also developed and submitted recommendations to E-ISAC on how to categorize, assess, disclose, and disseminate threat information that is most useful to public power utilities to avoid future threat information fatigue.

The secure information sharing platforms ensure that public power utilities are not overwhelmed by the deluge of information produced by intelligence sources. Eventually, given the ever-increasing volume of data, threat indicator sharing will need to move to an automated platform.

### NEXT STEPS

- Continue research with the National Laboratories and universities to pilot a Public Power Secure Information Clearinghouse tool which can provide better real-time information flow among E-ISAC, the Association, and utilities.
- Evaluate other secure information sharing technologies to integrate automated indicator data.

## Information Assurance

The Association researched recommended methodologies, best practices, and technologies to improve information assurance for data-in-motion. It developed webinars, a PowerPoint slide deck, and a report on three case studies of information assurance implementation at small, medium, and large public power utilities.

### NEXT STEPS

- The Association will work with joint action agencies to research whether aggregation of smart grid deployments at the agencies can ensure data protection.

Questions? Contact Nathan Mitchell, cybersecurity program manager, at NMitchell@PublicPower.org.

# Appendix A
# Cybersecurity Program Year 1 Participants

Adrian Public Utilities
Alabama Municipal Electric Authority
ALP Utilities
Alton Municipal Utilities
American Municipal Power, Inc.
Atlantic Municipal Utilities
Barbourville Utility Commission
Barnesville Municipal Utilities
Beaches Energy Services
Benson Municipal Utilities
Berea Municipal Utilities
Beresford Municipal Utilities
Boscobel Utilities
Bountiful Power
Bowling Green Municipal Utilities
Breckenridge Public Utilities
Breese
Brigham City
Bristol TN Essential Services
Brookings Municipal Utilities
Bryan Texas Utilities
Cameron
Carthage Water Electric
Central Municipal Power Agency/Services
Central Nebraska Public Power & Irrigation District
Central Utah Water Conservancy District
Chelan County PUD
Chillicothe
City of Albany
City of Charlevoix
City of Columbia
City of Fallon
City of Fulton
City of Higginsville
City of Lakota
City of Lindsborg
City of Marshall
City of McPherson
City of Memphis
City of Moberly
City of Monett
City of Ocala Electric Utility
City of Olivia
City of Paris Combined Utilities
City of Piqua
City of Purcell
City of Salem Electric Department
City of Seguin
City of Staples
City of Vermillion
City of West Plains
City of Williamstown
Clatskanie People's Utility District
CMUA
Coldwater Board of Public Utilities
Columbus Division of Power
Crisp County Power Commission
CUWCD
Delano Municipal Utilities
Denison Municipal Utilities
Denton Municipal Electric
Detroit Lakes Public Utilities
Electric Cities of Georgia
Electrical District No. 3 of Pinal County
ElectriCities of NC
Energy Northwest
Fairview City
Fallon Municipal Electric System
Fellmore City
Flandreau Municipal Utilities
Florida Municipal Power Agency
FMEA
Fort Pierce Utilities Authority
Frankfort Electric & Water Plant Board
Fulton
Gainesville Regional Utilities
Garland Power & Light
Grand Haven
Great Lakes Utilities
Guam Power Authority
Hannibal BPW
Harlan Municipal Utilities
Harrisonville
Hartley Municipal Utilities
Heartland Consumers Power District
Heber Light & Power

This material is based upon work supported by the Department of Energy under award number DE-OE0000811.

## Appendix A
## Cybersecurity Program Year 1 Participants

Henderson Municipal Power & Light
Hillsboro Electric Utility
HMU
Holland Board of Public Works
Homestead Energy Services
Hopkinsville Electric System
Hurricane City Power
Hyrum City Power
Idaho Falls Power
Illinois Municipal Electric Agency
Independence Power & Light
Indiana Municipal Power Agency
Jackson
Jackson Center Municipal Electric System
Kansas City Board of Public Utilities
Kansas Municipal Utilities
Kaysville City
Kentucky Municipal Power Agency
Kentucky Municipal Utilities Association
Kerrville Public Utility Board
Keys Energy Services
Kirkwood Electric
KMU
LADWP
Lake Park Public Utilities
Lakefield Public Utilities
Lakeland Electric
Lakota Municipal Utilities
Lawrenceburg Municipal Utilities
Lebanon Utilities
Lehi City
Lincoln Electric System
LMUD
Lodi Electric Utility
Logan City
Long Island Power Authority
Loup Power District
Lower Valley Energy
Luverne Municipal Utilities
Madison Municipal Utilities
Madisonville Municipal Utilities
Marshall Municipal Utilities
Marshfield Utilities
Mason County PUD #1
MEAG Power
Melrose Public Utilities
Memphis Light, Gas and Water
MEUW
Michigan Public Power Agency
Michigan South Central Power
Michigan South Central Power Agency
Mid-West Electric Consumers Association
Minnesota Municipal Utilities Association
Missouri Joint Municipal Electric Utility Commission
Missouri Public Utility Alliance
Missouri River Energy Services
Monroe City Power
Moorhead Public Service
Murray City
Murray Electric
MYMEAC
Nebraska City Utilities
Nebraska Public Power District
New London Electric & Water Utility
New Ulm
Nixa Municipal Electric System
North Attleboro
North Branch Municipal Water and Light
Northern California Power Agency
Northern Municipal Power Agency
Norwich Public Utilities
NTUA
NYAPP
Odessa
Oklahoma Municipal Power Authority
Omaha Public Power District
Orange City Municipal Utilities
Owatonna Public Utilities
Owensboro Municipal Utilities
Paducah Power System
Parowan
Paullina Municipal Utilities
Pella Municipal Electric Utility
Pierre Municipal Utilities
Piqua Municipal Power System
Platte River Power Authority

## Appendix A
## Cybersecurity Program Year 1 Participants

Princeton Electric Plant Board
Remsen Municipal Utilities
Rice Lake Utilities
Riverside Public Utilities
Rochester Public Utilities
Rock Rapids Municipal Utilities
Rolla Municipal Utilities
Russellville Electric Plant Board
Sanborn Municipal Utilities
Santee Cooper
Sauk Centre Public Utilities
SDMEA
SESD
Shelby Municipal Utilities
Sikeston BMU
Sioux Center Municipal Utilities
Southern Minnesota Municipal Power Agency
Southwest Public Power Agency
Springfield
Springville City
St. George City
St. James Public Utility
Utah Associated Municipal Power Systems
Valley City Public Works
Village of Sherburne Municipal Utilities
Washington City
Watertown Municipal Utilities
Waverly Utilities
Weber Basin Water Con
West Memphis
Westbrook Public Utilities
Westerville Electric Division
Willmar Municipal Utilities
Wilson
Woodbine Municipal Light & Power
Worthington Public Utilities
WPPI Energy
Zeeland Board of Public Works

AMERICAN PUBLIC POWER ASSOCIATION™
Powering Strong Communities

2451 Crystal Drive
Suite 1000
Arlington, VA 22202-4804
PublicPower.org