AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

Public Power Joint Action Agency Cybersecurity Services Plan

DECEMBER 2019

Acknowledgment

This material is based upon work supported by the Department of Energy under Award Number(s) DE-OE0000811.

Disclaimer: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

The American Public Power Association thanks the members of the Joint Action Agency Advisory Council for Cybersecurity (JAC-C), and other important contributors, for their role in developing this plan. The Council developed this plan to arm joint action agencies (JAAs) with cybersecurity services to offer their members in order to bolster the cyber defense of the public power industry. We thank the Council for taking the time to attend workshops and conference calls to share their experiences, needs, and practices. Everyone that contributed to this plan deserves thanks and appreciation.

Members of the Council included:

Brooke Carroll, Kansas Power Pool

Chris Ching, American Public Power Association

Sallie Coleman, Electric Cities of Georgia

Kevin Fulks, Missouri Public Utility Alliance

Branndon Kelley, American Municipal Power, Inc.

Christopher Kelley, Beam Reach Consulting Group

Joni Livingston, Missouri River Energy Services

Carter Manucy, Florida Municipal Power Agency

Nathan Mitchell, American Public Power Association

Mark Mraz, Beam Reach Consulting Group

Brittany Pouliot, American Public Power Association

Jared Price, American Municipal Power, Inc.

John Quan, Southern California Public Power Association

Sam Rozenberg, American Public Power Association

Chris Schoenherr, Southern Minnesota Municipal Power Agency

Brian Sharman, Beam Reach Consulting Group

Ben Slager, Wisconsin Public Power, Inc.

Other contributors:

Josh Cox, City of Westerville Electric Division

Tony Holstein, Gainesville Regional Utilities

Chris Lindell, Beatrice City Board of Public Works

Robby McCutcheon, Kerrville Public Utility Board

Doug Landoll, Beam Reach Consulting Group

Gareth Williams, Beam Reach Consulting Group

Helana Zagami, Beam Reach Consulting Group

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

About the Association

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.

Table of Contents

Executive Summary

Cybersecurity is a real and growing threat for public power utilities. Adversaries may be foreign or domestic, sophisticated or novice, and motivated by simple greed or a desire to cause havoc or political disruption. No utility is too small to be targeted, no municipality too limited in resources, no community too obscure to be overlooked, and no network completely secure.

Because of this multifaced and evolving threat, public power utilities need affordable access to comprehensive and expert resources. The most viable solutions are for a utility to develop a cybersecurity capability in-house or within a city department, or for a utility to contract with a vendor to provide direct support. However, many public power utilities simply lack sufficient financial means to pursue either of these solutions.

For the small to medium public power utility, cybersecurity services and resources are available, but few are developed to address challenges specific to these utilities. For example, the threat alerts published by government and commercial organizations are not tailored or customized for use by public power organizations.

In response, the American Public Power Association (Association) chartered the Joint Action Agency Advisory Council for Cybersecurity (JAC-C) to make recommendations to improve public power's cybersecurity posture. The JAC-C proposed the Public Power Cybersecurity Enhancement Framework (Framework), which details a structure to provide cyber resources to utilities from three parts of the public power ecosystem: the Association, joint action agencies (JAAs), and super JAAs.

Due to the magnitude of the public power sector nationwide — thousands of utilities ranging in size, scope, and personnel profile — the Association relies on JAAs to work closely with their constituent utilities. The Association coordinates at a national level while JAAs and super JAAs provide tailored support at the regional and local levels. Given this, the JAC-C identified that JAAs are in a unique position to be most effective at influencing the improvement of cybersecurity at the utility level.

The Framework identifies the following roles and services, in aggregate, which are needed to provide relevant knowledge and abilities to improve utilities' preparation for and response to threats.

Important roles in this endeavor include:

- Cybersecurity Program Manager: an advocate and resource for public power cybersecurity
- Open Source Threat Analyst: a central source that collects, analyzes, disseminates, and makes recommendations on threat information specifically for public power
- Technical Advisor: an on-call trusted resource for the utility-level cybersecurity specialist
- Cyber Insurance Review: a resource for evaluating, selecting, acquiring, and using cyber insurance products for public power

Services the Association, a JAA, or super JAA can offer/secure for utilities include:

- Incident Response: an organized approach to addressing and managing the aftermath of a cyberattack
- Security Assessment: helping public power utilities to determine appropriate assessments and on how to find and contract with an appropriate resource, including local or national consultancies
- Cybersecurity Exercises: assess and strengthen a utility's ability to detect, analyze, respond, and recover from a cyber threat
- Cybersecurity Training: provide employees with the information and techniques to protect their networks from cyberattack

Cybersecurity Services for Public Power

Cybersecurity Services	Lead	APPA	JAA	Super JAA
Program Management	**APPA**	• Find new ideas, technology • Liaise w/national orgs • Outreach to public power • Develop vision & strategy • Centralize information • Coordinate w/threat analyst		
Open Source Threat Analysis	**APPA**	• Collect all threat dat • Distribute tailored report • Make recommendations • Liaise w/national orgs • Work w/program manager	• Identify IT/OT Hardware • Analyze tailored reports • Make recommendations • Liaise w/threat analyst	• Identify IT/OT Hardware • Analyze tailored reports • Make recommendations • Liaise w/threat analyst
Technical Advice	**Super JAA or JAA**	• Link to national resources	• On-call resource for utility • Advise on cyber IT/OT issues • Liaise w/program manager • Review threat reporting	• On-call resource for utility • Advise on cyber IT/OT issues • Liaise w/program manager • Review threat reporting
Cyber Insurance Trusted Advisor	**Super JAA or JAA**	• Publish a white paper on cyber insurance for public power • Provide training seminars to JAAs on cyber insurance for public power	Advise selection of relevant insurance: • Evaluate need • Review types of insurance • Select and acquire insurance • Make a claim • Account for special considerations	Advise selection of relevant insurance: • Evaluate need • Review types of insurance • Select and acquire insurance • Make a claim • Account for special considerations
Incident Response	**Super JAA or JAA**	• Response Playbook • Link to national resources	• On-call assist for cyberattack • Create incident response plan • Manage incident response • Link to resources	• On-call assist for cyberattack • Create incident response plan • Manage incident response • Link to resources
Security Assessment	**Super JAA or JAA**	• Scorecard • Onsite assessments	• Provide services: • Risk Assessment • Social Engineering • Penetration Testing • Vulnerability Scanning	• Provide services: • Risk Assessment • Social Engineering • Penetration Testing • Vulnerability Scanning
Cybersecurity Exercise	**JAA**	• Link to national exercise	• Evaluate exercise needs • Plan & manage exercises • Evaluate performance • Provide lessons learne	
Cybersecurity Training	**JAA**	• Conferences • Workshops • Association Academy	• Conferences • Workshops • Association Academy	• Conferences • Workshops • Association Academy

The Association, JAAs, or super JAAs can also assist utilities with identification, selection, and vetting of vendors to supplement their technology, skills, and experience..

To gauge progress at the utility and industry levels, and to aid continual improvement, the Association, JAAs and super JAAs will need to develop and capture a similar set of metrics. To reinforce the needs of the program to funding and other relevant agencies, these metrics must capture the benefits of the program and improvements to utility cybersecurity. The JAC-C proposed a set of metrics to track the effectiveness of the Framework. These include Cybersecurity Performance Assessment metrics and Cybersecurity Program metrics.

Cybersecurity Performance Assessment metrics capture the impact of the program on a utility and improvements to its operations. These include network detection and intrusion; device security; account security; logging and monitoring; risk management; security awareness; vendor management; and incident response.

Cybersecurity Program metrics assess the impact of the cybersecurity services program offered by the Association, JAA, or super JAA. These might include: member improvement in the Cybersecurity Performance Assessment metrics, membership retention, most and least valuable services offered, adoption of services, and return on investment.

To help JAAs and super JAAs determine if and how to offer the services in this Framework to members, each should create an execution plan addressing the baseline criteria layed out in the chart below..

Ultimately, the success of these programs will depend on both the diligence of the Association, JAAs, and super JAAs, and the initiative and commitment of utilities nationwide.

Public Power Cybersecurity Services Execution Plan Criteria

Leadership and Workforce	Financial	Marketing	Resourcing
• Study plan to gain insights • Conduct preliminary discussions with leadership group • Share plan with stakeholders and gather feedback • Evaluate feedback and develop a change management plan • Gain leadership group approval to proceed • Formalize sustainment structure charter	• Gain better understanding of the market • Create marketing materials for consumers • Segment market: mature, immature, hybrid • Assess benefits to JAA/ Super JAA and consumers: direct, indirect • Survey potential consumers on interest and demand	• Develop a financial model • Determine a payment structure: dues, per service, other • Develop a pro-forma financial analysis • Estimate costs for cyber services • Determine price tolerances	• Assess whether to resource internally or externally • Conduct Build vs. Buy analysis for services • Analyze competitors or partners for each service • Vet and contract with vendors • Hire and train internal staff • Conduct quality assurance

Introduction

The U.S. power grid is the largest machine on Earth and delivers $400 billion worth of electricity each year to government, business, and residential customers.[1] Reliable and coordinated operation of this massive, interconnected machine is increasingly dependent on computing technology. This reliance on computing technology has become an infrastructure Achilles' heel and makes it a prominent target of foreign governments, third-state actors, and criminal and terrorist organizations. For instance, in June 2019, the New York Times published an article citing high-ranking U.S. government sources that alleged Russian hackers targeted the U.S. power grid and conducted reconnaissance of electrical power information and operations technology systems.[2]

In 2017, President Trump issued Executive Order 13800, which directed the U.S. government to strengthen the cybersecurity of critical energy infrastructure as a national security imperative.[3]

Amid the ever-growing threat of cyberattack, public power entities are challenged to safeguard networks and to develop a culture of cybersecurity.

Strengthening Public Power's Cybersecurity

In 2016, the American Public Power Association (Association) entered a three-year cooperative agreement with the U.S. Department of Energy (DOE) "to improve the cyber resiliency and cyber security posture of public power utilities."[4] As part of this agreement, the

Association chartered two committees to address the challenges of improving public power cybersecurity programs: the Cybersecurity Resource Advisory Committee (CRAC) and the Joint Action Agency Advisory Council for Cybersecurity (JAC-C).

JAC-C includes personnel from the Association, representatives of JAAs, and other trusted partners in the public power industry. The council's purpose is to develop collaborative solutions to address the cyber threat to public power. JAC-C held eleven meetings between June and November 2019 focused on developing this plan, including an in-person summit at the Association's office in Arlington, Virginia on September 19, 2019.

Leveraging Joint Action for Cybersecurity

Joint Action Agencies (JAAs) are a pivotal cog in organizing and equipping public power utilities to bolster cybersecurity across the industry. Historically, JAAs were established to purchase bulk power for groups of utilities at a reduced rate, provide for generation services, or to perform quantity purchase of goods and services for their members. The role of the JAA has since evolved. The ability of JAAs to organize utilities, and their established relationships with their member utilities, make them key influencers in public power. Further, in most cases, JAAs have developed shared resources that may be useful to confront cyber threats.

There are more than 2,000 public power utilities in the United States.[5] All public power utilities are at risk of cyberattack and are therefore a potential consumer of cybersecurity services.

Given this broad footprint, it would be unwieldy for a single entity like the Association to develop and manage cybersecurity services for all public power utilities.[6] On average, a JAA serves approximately 20 public power utilities. Given this ratio, JAAs are better positioned to disseminate and influence cybersecurity best practices at their member utilities.

Through JAC-C, the Association and the JAAs together can reduce public power utilities' barriers to adopting cybersecurity best practices. To bolster cybersecurity for their members, JAAs need to develop, offer, and manage cybersecurity services at the utility level. This plan outlines how JAAs can acquire the capabilities to address cybersecurity threats that can be offered as a member service.

Challenges and Recommended Solutions

Approximately 700 public power utilities use both information technology (IT) and operational technology (OT) systems to conduct business. As the public power industry has increased reliance on OT and IT systems and broadened its risk silhouette, federal government and industry have sought to provide solutions.

From March to June 2019, the Association conducted interviews of cybersecurity specialists at the utility- and JAA-level. Utility-level cybersecurity specialists acknowledged that cyber threats were a critical concern at their utility. Moreover, all respondents stated they had demand for additional cybersecurity services to bolster cyber defense. Our research and interviews determined that most utilities lack the resources and technical capability to develop a cyber incident response plan, track threats, harden networks, or respond to a cyberattack absent third-party assistance.

Respondents vocalized support for the concept of having a JAA offer cybersecurity services for member utilities. Our research and interviews identified gaps in cybersecurity services tailored for public power utilities. Interviewees expressed demand for the following eight specific services: program management, open source threat analysis, technical advice, incident response, vulnerability assessment, vulnerability exercises, training, and cyber insurance trusted advisor.

Plentiful Information, Limited Resources

Many public power utilities have a small cybersecurity workforce tasked to perform multiple duties. In some cases, this workforce may be one employee. In other cases, employees in other city departments may be tasked with tackling cybersecurity duties. For the most part, this workforce does not have the time to collect, read, analyze, and respond to the large volume of threat alerts published by the commercial industry and by government agencies at the federal, state, and local level. At an Association event, the Multi-State Information Sharing and Analysis Center (MS-ISAC) noted that it published more than 300 threat alerts in 2018.

Furthermore, threat alerts published by government and commercial organizations are not tailored or customized for use by public power organizations. Resources are available to address cyber threats, but few are developed to address challenges specific to the small to medium public power utility.

The most viable solutions are for a utility to develop a cybersecurity capability in-house or within a city department, or for a utility to contract with a vendor to provide direct support. The latter alternative might be feasible for large public power utilities with the financial resources to enlist a vendor to safeguard its networks. However, many public power utilities simply lack sufficient financial means.

Recommended Solution

To address these cybersecurity challenges from the macro level at each link of the public power industry, the JAC-C developed the Public Power Cybersecurity Enhancement Framework (Framework).

The Framework looks at offering cyber resources to utilities from three parts of the public power ecosystem: The Association, JAAs, and super JAAs (consortia of JAAs and vendors with special resources, skills, experience, and relationships with third parties).[7]

Cybersecurity services should be offered at three points in the public power enterprise: the Association, JAAs, and super JAAs. We describe each of the three components below.

Activities

American Public Power Association

The Association has three years of experience with developing, coordinating, and implementing cybersecurity services for public power nationwide via a cooperative agreement with the DOE. The agreement has enabled the Association to organize, train, and equip the public power industry with resources and services needed to prepare for a cyber incident. The Association is the primary conduit for public power to the Executive and Legislative Branches of the U.S. government. In this capacity, the Association advocates for funding, legislation, and federal support for public power.

JAAs

JAAs are the primary building block of this plan. Each JAA is a consortium of public power systems within a state, or specific geographic area. The 100 JAAs spread across the United States are intertwined with the 2,000+ public power utilities. No single link in the public power enterprise has a larger touch point with the utilities than the JAA. In most cases, a JAA has the resources, skills, and relationships with third parties exceeding that of small, medium, and many large-sized utilities.

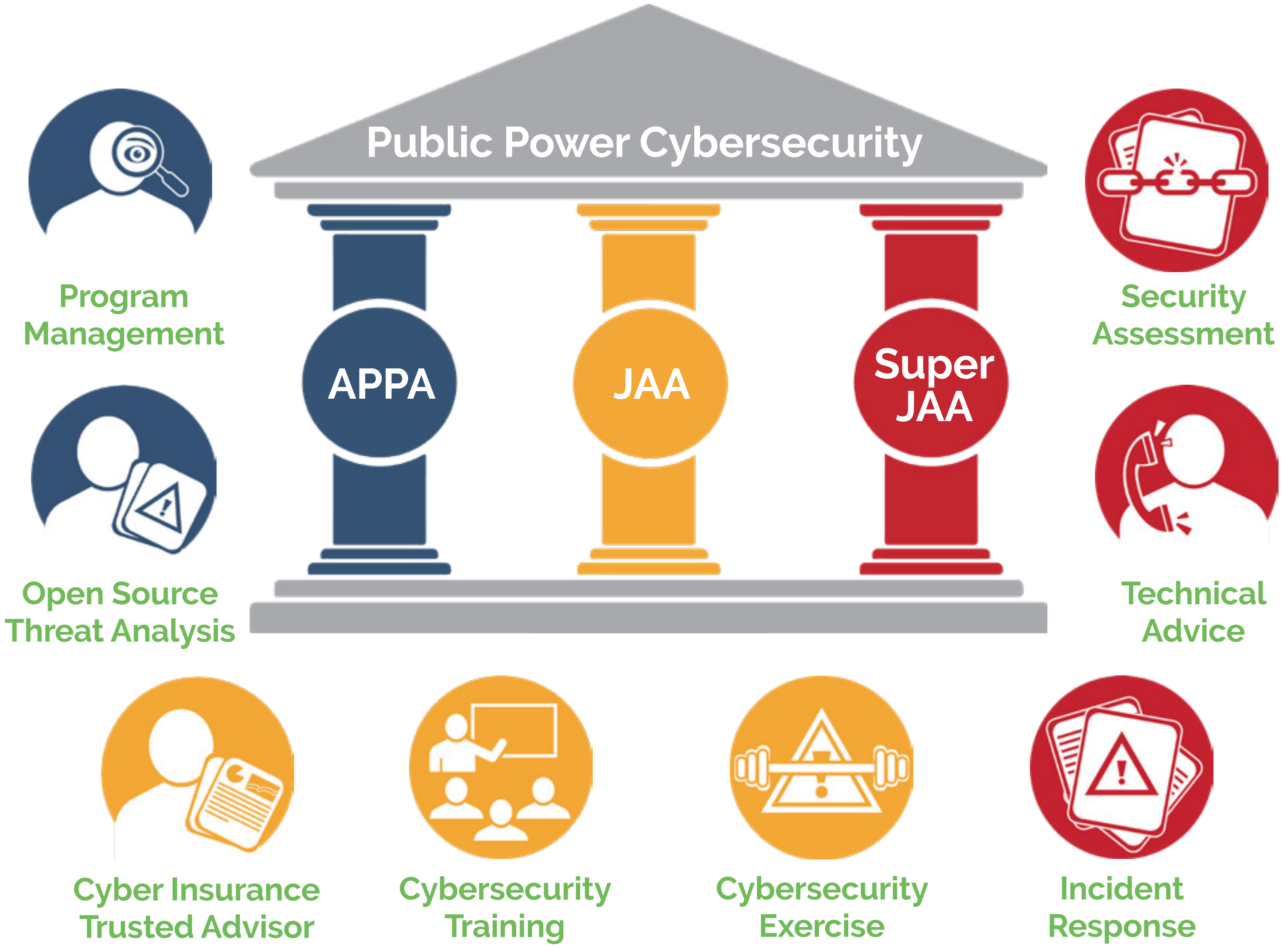
Super JAAs

A super JAA is a consortium of JAAs and vendors with special resources, skills, experience, and relationships with third parties. A super JAA is not confined to a state or geographic area. A super JAA may provide services at a regional or national level. Super JAAs typically provide services to more public power entities than JAAs, which might be constrained by charter mandates or bylaws.

These three entities are all conduits to the individual utility and can consider developing and offering the following eight cybersecurity services.[8] We identify and define the scope of those services as follows, however, a JAA can consider how to tailor these services to best meet its members' needs.

Public Power Cybersecurity Enhancement Framework

This model outlines the cybersecurity services designed to support public utilities' efforts to improve cybersecurity. The framework incorporates roles from APPA, JAAs, and Super JAAs alike.



Cybersecurity Services

The Association, JAAs, and super JAAs each will provide services to support public power utilities' efforts to improve cybersecurity. These services will be the responsibility of several positions, each addressing different needs at local to national levels of coordination. An overview of these services, position responsibilities, and relevant knowledge and skills is detailed below.

Program Management (National)

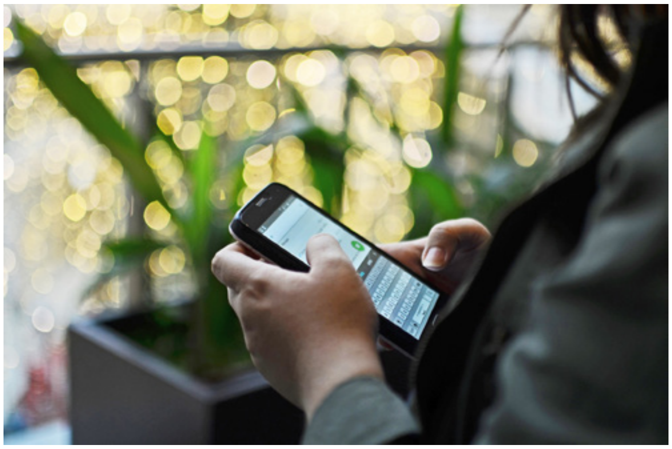
Description: Advocate and resource for cybersecurity in the public power industry.

Responsibilities:

- Develop a public power cybersecurity vision and strategic plan
- Study government and industry for best practices, vendors, processes, and tools to improve cybersecurity
- Coordinate cybersecurity resources and tools for all public power providers
- Outreach to the public power community through meetings, information sharing activities, and strategic communication
- Consolidate information from a variety of government and non-government sources for more efficient use by public power utilities
- Assist in coordinating and deconflicting unity of effort among the Association, JAAs and super JAAs
- Liaise and advocate for public power with federal and national organizations such as the Department of Energy, Department of Homeland Security, Federal Energy Regulatory Commission, Electricity Information Sharing and Analysis Center (E-ISAC), Multi-State Information Sharing and Analysis Center (MS-ISAC), and the National Institute of Standards and Technology (NIST)

Critical Knowledge, Skills, and Abilities:

- Knowledge of and experience with public power organizational structures and awareness of contemporary cybersecurity issues and responses that impact public power.
- Knowledge of the Public Power Cybersecurity Enhancement Framework.
- Awareness of public power industry service organizations and experience interacting with these organizations to deliver successful programs.
- Program management skills and the ability to manage, communicate, and organize cybersecurity resources, tools, and liaisons from within the public power industry



Open Source Threat Analysis (National)

Description: The central figure in collecting, analyzing, disseminating, and making recommendations on threat information to the public power industry.

Responsibilities:

- Collect and analyze all threats to public power reported by government and non-government sources[9]
- Consolidate reporting into a clear and succinct information stream tailored for public power utilities
- Produce and disseminate actionable threat information that makes recommendations for decision makers
- Coordinate outreach to the public power industry with the Cybersecurity Program Manager
- Liaise with information sharing agencies such as MS-ISAC and E-ISAC
- Liaise and advocate for public power with federal and national organizations such as DOE, DHS, FERC, E-ISAC, MS-ISAC, and NIST
- Maintain a secret-level security clearance to receive briefings from intelligence and law enforcement agencies

Critical Knowledge, Skills, and Abilities:

- Knowledge of contemporary cybersecurity issues and responses that impact public power.

- Awareness of public power planning and operational practices to filter and prioritize cybersecurity threats unique to public power.
- Deep understanding of cybersecurity threat intelligence, threat intelligence sources, current methods of dissemination, threat feed techniques, and threat advisory contents
- The ability to write, present, and communicate effectively; the ability to review, research, confirm, and determine appropriateness of cybersecurity threats to the public power industry

Technical Advice (State/Local)

Description: An on-call trusted resource for the utility-level cybersecurity specialist.

Responsibilities:

- Assist utility-level cybersecurity specialists on IT and OT security issues
- Advise utility-level cybersecurity specialists on program initiatives such as assessment, policy development, product selection, risk management, security metrics, and awareness training
- Provide continuing education to utilities related to emerging threats, trends, and new technology
- Maintain close ties with the Cybersecurity Program Manager and Open Source Threat Analyst

Critical Knowledge, Skills, and Abilities:

- Ability to work remotely and travel on-site, as needed
- 3–5 years of experience working in the public power industry
- 3–5 years of experience working in cybersecurity
- Certified Information Security System Professional (CISSP) or Certified Information System Manager (CISM)]
- Experience in incident handling, investigation, and remediation, including relevant open source tools and techniques, such as:[10]
    - Log analysis (Open Source Security Information and Event Management [OSSIM])
    - Intrusion detection systems (Snort, Open Source Security Event Correlation [OSSEC])
    - Network flow analyzers (ntopng, Nfdump)
    - Vulnerability scanners (Open Vulnerability Assessment System [OpenVAS], Nessus)
    - Availability monitoring (Nagios)
    - Web proxies (Squid Proxy, IP Fire)
    - Asset inventory (Open Computer Software [OCS] Inventory)
    - Threat intelligence (Alien Vault Open Threat Exchange [OTX], Open Source Security Information Management [OSSIM])
    - Data capture (SANS Investigative Toolkit [SIFT], SleuthKit, Autopsy)
    - System backup, patch management (Open PC Server Integration [OPSI])

Cyber Insurance Trusted Advisor (National/State/Local)

Description: A resource with targeted knowledge for evaluating, selecting, acquiring, and using cyber insurance products in the public power industry.

Responsibilities:

- Advise utility-level specialists on the scope of cyber insurance and how to evaluate need
- Advise utility-level specialists on the availability of cyber products in the industry and the special considerations associated with selecting and acquiring products
- Advise utility-level specialists on how to make a cyber insurance claim and the special considerations associated with that process

Critical Knowledge, Skills, and Abilities:

- Experience working in the public power industry
- Knowledge of physical and cyber insurance products available to public power

Incident Response (National/State/Local)

Description: An on-call trusted resource for their members subsequent to a cyberattack. Incident response provides an organized approach to addressing and managing the aftermath of a cyberattack.

Responsibilities: Develop an incident response program for members.

- Create a tailored incident response plan for each utility
    - Log Inventory and document cyber assets
    - Inventory and document cyber assets
    - Record the network architecture
    - Identify key personnel needed to respond to an incident
    - Develop resources needed to respond to an incident
    - Liaise with third parties needed to assist with an incident
- Advise on logging, system monitoring, and threat monitoring for incident identification capabilities
- Advise on staff capabilities, training, and access to vendors for creation of an incident response team
- Manage incident recovery and after-action review and posturing

Critical Knowledge, Skills, and Abilities:

- Knowledge of regulations and laws governing notification of data disclosures and breaches
- Skilled at the remediation, recovery, and response approaches for various cyber security incidents
- Able to communicate effectively

- Incident handling certifications (Global Information Assurance Certification – Certified Incident Handler [GCIH], EC-Counsel Certified Incident Handler [ECIH], Certified Expert Incident Handler [CEIH])
- 3–5 years of experience in cyber incident response

Security Assessment (State/Local)

Description: Security assessments are objective reviews or tests of an organization's security controls. These assessments can be applied to various controls, involve different techniques, and be governed by increasing levels of rigor. These services may be acquired from local or national consultancies.

Responsibilities:

- Advise public power utilities on the availability, scoping, contracting, and overseeing of security assessment services
- Create standard SOW templates for each of the services listed
- Define recommended service frequency and pricing parameters
- Determine appropriate resources, tools, and techniques for those public power utilities wanting to provide this service for internally
- Determine the appropriateness of standing up a local or regional capability to offer these services to public

power utilities

Description: Devise and administer a process for identifying, analyzing, and addressing potential vulnerabilities in IT and OT system controls. Typical and appropriate security assessment services for public power utilities include:

- Security risk assessment of IT and OT systems
- Assessment of social engineering (phishing, pre-texting, etc.) vulnerabilities
- Penetration testing of networks and web applications
- Vulnerability scanning
- Wireless security review

At the JAA level, this service could involve advising and assisting public power utilities in how to determine which assessments are appropriate for the utility to conduct and how to find and contract with an appropriate resource. The service could entail:

- Advising on the market needs as well as the availability, scoping, contracting, and overseeing of security assessment services
- Creating scope of work templates for each of the services listed
- Defining recommended service frequency and pricing parameters
- Determining the appropriate resources, tools, and techniques for public power utilities wanting to conduct assessments internally

Cybersecurity Exercise (National/State/Local)

Description: Cybersecurity exercises assess a utility's ability to detect, analyze, respond, and recover from a cyber threat. The cybersecurity maturity of the public power community encompasses a wide range of abilities and knowledge. However, many small- to medium-size utilities are in the infancy of developing and implementing cybersecurity programs. Thus, exercises should be tailored to the utility's levels of cybersecurity maturity

Lower Cybersecurity Maturity

- Introduce the concept of an incident response plan and conduct a tabletop exercise that guides utility personnel through the process
- Participate in events like GridEx as an observer

Higher Cybersecurity Maturity

- Actively participate in the North American Electric Reliability Corporation (NERC) Grid Security Exercise (GridEx)
- Simulate a cyberattack in which the utility's incident response plan is triggered

Responsibilities: Exercise planners should:

- Define objectives, parameters, and schedule for the exercise
- Create scenarios, exercise material, and identify exercise elements (the Association has sample scenarios and template materials available)
- Identify and manage exercise logistics
- Facilitate the exercise and ensure an evaluation is recorded
- Create and distribute a lessons-learned report

Cybersecurity Training (National/State/Local)

Description: Cybersecurity training provides employees with the information and techniques to practice good security hygiene and to protect networks from cyberattack. A variety of types of training courses would be useful for three audience groups: 1) all public power utility staff, 2) network and SCADA operators, and 3) cybersecurity specialists. The table below includes examples of training for each of these three groups.[11]

Level 1: All utility staff	Level 2: OT and network operators	Level 3: Cybersecurity Specialists
All employees require basic cyber awareness training, such as: • SANS Security Essentials • KnowB4 • ProofPoint • Ninjio • Cofense • Infosec IQ • Defence Works • Habitu8	Engineers that are in contact with OT devices and networks require an additional level of training, such as: • SANS Managed Security for OT Networks	Utility cybersecurity specialists require specialized cyber training to manage OT and IT networks, such as: • Certified Information Systems Security Professional (CISSP)

Cybersecurity Services for Public Power

JAC-C explored the appropriate place to house each of these services among the Association, JAAs, and Super JAAs. After much discussion, we suggest that many of the services have elements provided by all three. The table on the next page outlines recommended responsibilities for each service.

Cybersecurity Services for Public Power

Cybersecurity Services	Lead	APPA	JAA	Super JAA
Program Management	**APPA**	• Find new ideas, technology • Liaise w/national orgs • Outreach to public power • Develop vision & strategy • Centralize information • Coordinate w/threat analyst		
Open Source Threat Analysis	**APPA**	• Collect all threat dat • Distribute tailored report • Make recommendations • Liaise w/national orgs • Work w/program manager	• Identify IT/OT Hardware • Analyze tailored reports • Make recommendations • Liaise w/threat analyst	• Identify IT/OT Hardware • Analyze tailored reports • Make recommendations • Liaise w/threat analyst
Technical Advice	**Super JAA or JAA**	• Link to national resources	• On-call resource for utility • Advise on cyber IT/OT issues • Liaise w/program manager • Review threat reporting	• On-call resource for utility • Advise on cyber IT/OT issues • Liaise w/program manager • Review threat reporting
Cyber Insurance Trusted Advisor	**Super JAA or JAA**	• Publish a white paper on cyber insurance for public power • Provide training seminars to JAAs on cyber insurance for public power	Advise selection of relevant insurance: • Evaluate need • Review types of insurance • Select and acquire insurance • Make a claim • Account for special considerations	Advise selection of relevant insurance: • Evaluate need • Review types of insurance • Select and acquire insurance • Make a claim • Account for special considerations
Incident Response	**Super JAA or JAA**	• Response Playbook • Link to national resources	• On-call assist for cyberattack • Create incident response plan • Manage incident response • Link to resources	• On-call assist for cyberattack • Create incident response plan • Manage incident response • Link to resources
Security Assessment	**Super JAA or JAA**	• Scorecard • Onsite assessments	• Provide services: • Risk Assessment • Social Engineering • Penetration Testing • Vulnerability Scanning	• Provide services: • Risk Assessment • Social Engineering • Penetration Testing • Vulnerability Scanning
Cybersecurity Exercise	**JAA**	• Link to national exercise	• Evaluate exercise needs • Plan & manage exercises • Evaluate performance • Provide lessons learne	
Cybersecurity Training	**JAA**	• Conferences • Workshops • Association Academy	• Conferences • Workshops • Association Academy	• Conferences • Workshops • Association Academy

Metrics

Good cyber hygiene requires diligent, ongoing practice – which can be underscored by meaningful measures of program success. Metrics allow decision makers and those responsible for performance to gauge progress and provide clear direction to others. Therefore, metrics that indicate completion are less relevant than those that provide guidance over time. JAC-C proposed a set of metrics to track the effectiveness of the framework proposed in this document. These include **Cybersecurity Performance Assessment** metrics and **Cybersecurity Program** metrics.

Cybersecurity Performance Assessment

Metrics that grid operator organizations already use contribute value to ongoing operations. Examples include System Average Interruption Duration Index (SAIDI), System Average Interruption Frequency Index (SAIFI), and Customer Average Interruption Duration Index (CAIDI). Cybersecurity metrics address a similar need as these operational measures (e.g., ongoing safety, reliability). A uniform format for metrics would allow useful analysis across organizations and regions. Additionally, by linking cybersecurity metrics to existing strategic metrics for public power entities, improvements in cybersecurity can be shown to contribute to overall organizational performance.

Small Vulnerabilities Cost Hundreds of Thousands of Dollars and Weeks of Effort

A cyber hacking incident occurs every 39 seconds in the United States, according to a University of Maryland study. Public agencies are attractive targets for cyber attacks, and smaller municipalities with limited resources for defense are particularly attractive for ransomware attacks, where the cyber attack encrypts essential data until the municipality provides a payment to the attacker.

In one case, an anonymous cyber-attack cost a small city nearly $100,000 in Bitcoin ransom and labor to recover from the attack. The attack likely demanded no more than a few minutes of the attacker's time but cost the city several weeks' work to clean up. After gaining access through a remote desktop host server, the attacker acquired an administrator password common to nearly every device on the network. The attacker then encrypted all data accessible through the administrator password, crippling the city's operations.

Subsequent investigation by city IT analysts, the state's National Guard cyber protection team, and the Department of Homeland Security determined the attack was from overseas and comparatively simple—a "script kiddie" or bot—because an SQL server running at the time was not compromised and could have been with a more sophisticated attack. Coordinated efforts over the next two weeks exchanged Bitcoin for the encryption key, which decoded all the files. The response team then worked for another month to restore and secure the remaining operations. The stark lesson being that this was not a particularly advanced or targeted attack, and it was able to incur significant disruption and expense.

Sources: [Cukier, Michel. "Study: Hackers Attack Every 39 Seconds." Clark School. February 9, 2007.]
[Small public power utility and municipality, name withheld at municipality's request]

JAC-C Suggested Cybersecurity Performance Assessment Metrics

Network Detection & Intrusions	Device Security
• Number of intrusion attempts (by severity) • Unidentified devices on network • Number of communication ports open	• Virus, Botnet, and other malware intrusions per device per month • Aging of critical patches
Logging and Monitoring	**Risk Management**
• Percentage of systems monitored • Number of events/alerts detected • Percentage of employees network usage monitored • Volume of data transferred on corporate network • Virus/malware statistics	• Aging of critical and high risks in risk register • Aging of assessment activities: risk assessment, penetration test, vulnerability scanning, social engineering
Vendor Management	**Incident Response**
• Number of exceptions in vendor risk management program • Percentage of vendors monitored • Frequency of review of vendor access • Percentage of vendor compliance with each of the vendor compliance requirements (e.g., CISO, Incident Response, penetration testing)	• Number of incident reports • Intrusion detection time (mean time to detect) • Intrusion response time • Intrusion remediation time (mean time to resolve)
Account Security	**Security Awareness**
• Dormant account aging • Number of super users • Aging of account rights reviews • Aging for terminated employee accounts • Percentage of weak passwords	• Phishing results • Social engineering results • Percentage of staff trained within the last 12 months

Cybersecurity Program Assessment

The JAC-C recommended that it continue to shepherd implementation of the framework. Once implemented, the owners of the program (including the Association, JAAs, and Super JAAs) should agree on ongoing performance metrics of the overall public power cybersecurity program. These metrics will be useful guides for improving and adjusting approaches recommended in the Public Power Cybersecurity Enhancement Framework. The JAC-C recommended metrics that assess:

- Member improvement in the Cybersecurity Performance Assessment metrics over time and correlated to services offered
- Membership retention
- Most and least valuable services offered
- Adoption of services
- JAA and Super JAA revenues and ROI

Next Steps

Armed with this plan, the JAC-C discussed and identified subsequent steps for JAAs and super JAAs to take to implement the services identified in this plan. These steps include development of an execution plan to assess and prioritize services identified in the Framework to members. The JAC-C recommends that the baseline criteria identified in the table below be addressed in an execution plan.

Execution Plan Baseline Criteria

Leadership and Workforce	Financial	Marketing	Resourcing
• Study plan to gain insights • Conduct preliminary discussions with leadership group • Share plan with stakeholders and gather feedback • Evaluate feedback and develop a change management plan • Gain leadership group approval to proceed • Formalize sustainment structure charter	• Gain better understanding of the market • Create marketing materials for consumers • Segment market: mature, immature, hybrid • Assess benefits to JAA/ Super JAA and consumers: direct, indirect • Survey potential consumers on interest and demand	• Develop a financial model • Determine a payment structure: dues, per service, other • Develop a pro-forma financial analysis • Estimate costs for cyber services • Determine price tolerances	• Assess whether to resource internally or externally • Conduct Build vs. Buy analysis for services • Analyze competitors or partners for each service • Vet and contract with vendors • Hire and train internal staff • Conduct quality assurance

Conclusion

JAA decision-makers and their members face cyber threats, which create potential for a new set of services. This document describes what the Association, JAAs, super JAAs, should consider in offering cybersecurity services to members.

By focusing on activities at the level best suited to respective operations, the Association, JAAs, super JAAs can work closely with utilities and provide tailored support at the local to national levels. Support services defined in this report identify where each entity in the public power enterprise can draw on expert personnel, tools, and resources to offer these resources. From planning and response advisors to insurance, the suite of services can improve both how a utility operates and how it prepares for or recovers from an attack.

By developing, offering, and measuring these resources, materials, and services, together we can foster a robust culture of cybersecurity in public power. Ultimately, the success of these programs will depend both on the diligence of the Association, JAAs, and super JAAs, and the initiative and commitment of utilities nationwide.

Appendix A: Resources, Notes and References

Resources

U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2): https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0

APPA Cybersecurity Resources page: https://www.publicpower.org/topic/cybersecurity

Public Power Cybersecurity Scorecard: https://www.publicpower.org/resource/cybersecurity-scorecard

For additional information on incident response, we recommend you review APPA's Cyber Incident Response Playbook which can be downloaded from: https://www.publicpower.org/resource/public-power-cyber-incident-response-playbook

References and Notes

1 Martin, Chris and Wade, Will. "America's Power Grid." Bloomberg, March 14, 2019. Accessed June 17, 2019. https://www.bloomberg.com/quicktake/u-s-electrical-grid

2 Sanger, David and Perlroth, Nicole. "U.S. Escalates Online Attacks on Russia's Power Grid." The New York Times, June 15, 2019. Accessed June 17, 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

3 U.S. Library of Congress, Congressional Research Service, Electric Grid Cybersecurity, R45312 (2018), ii.

4 U.S. Congress. House. Committee on Energy and Commerce. DOE Modernization: Legislation Addressing Cybersecurity and Emergence Response. March 14, 2018. Accessed July 11, 2019. https://docs.house.gov/meetings/ IF/IF03/20180314/107999/HHRG-115-IF03-20180314-SD054.pdf

5 2019 Public Power Statistical Report. Arlington, VA. American Public Power Association, 2019. Accessed November 26, 2019. https://www.publicpower.org/resource/2019-public-power-statistical-report

6 See, American Public Power Association website, "Our Members." Accessed July 11, 2019. https://www.public power.org/our-members

7 An example of a Super JAA is Hometown Connections, Inc. For more information, visit: https://www.hometownconnections.com/

8 The eight services were identified by the JAC-C, utility cybersecurity specialists, and JAA cybersecurity specialists. JAAs may choose to include additional services as they deem appropriate.

9 The JAC-C defined reporting as alerts from commercial and government organizations, reports from the national and local media, and data generated from the public power IT and OT systems. This list is not intended to limit additional inclusions, as the JAA determines is appropriate.

10 The open source tools list under the Technical Advice service was provided by the JAC-C for context about the types of resources that would be useful. This list is not exhaustive and may vary by regional and utility needs.

11 These training courses and certifications are provided as examples for context. The list is not exhaustive.

All photos courtesy of Pixabay

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

2451 Crystal Drive
Suite 1000
Arlington, VA 22202-4804

www.PublicPower.org

#PublicPower