Improving the Cyber Resiliency and Security Posture of Public Power

EXECUTIVE SUMMARY AND TECHNICAL APPROACH

The American Public Power Association (APPA) represents not-for-profit, community-owned electric utilities that power homes, businesses, and streets in nearly 2,000 towns and cities, serving 48 million Americans. More than half of all public power utilities have under 2,000 customers.

Public power distribution utilities may have unique organizational structures with regard to operations, systems control and monitoring, internal or city information technology departments, leadership/governance, and use of third party cyber security service providers. These structures may not lend themselves to a one size fits all approach to cyber risk assessment, threat information sharing or coordinated response to incidents. These nuances within the public power community may require tailored cyber security resources which may include risk assessment tools, threat information sharing processes, response and recovery plans and a better understanding of what technologies would work for the public power business model.

It is the intent of this multiyear/multi-faceted program to help public power utility managers improve their cyber resiliency and security posture. To achieve this goal APPA proposes to use an analytical risk assessment approach to better understand the needs of each public power community. Once the needs are known the program activities can then focus on tools of most use for public power managers as they decide how best to improve their cyber security posture.

Under the cooperative agreement APPA must undertake, at a minimum, four tasks, which include 1) Efforts to advance cyber resiliency and security assessments; 2) Conduct, evaluate, and use the results of on-site vulnerability assessments; 3) Research, evaluate, deploy, and integrate both commercial and pre-commercial security technologies; and 4) Research, evaluate, and implement information sharing mechanisms.

The purpose of completing these tasks is to write and disseminate educational resources, update guides, conduct training sessions, and undertake outreach efforts so utility managers can make informed decisions on implementing cyber security programs and deploying cyber security technologies. The objective of these strategies is to foster a cyber and physical resiliency and security culture at public power utilities. The educational materials may include reports, key findings from assessment results, case studies, meeting summaries, webinars, recommendations and frameworks to increase the resiliency and security capabilities of public power distribution utilities.

APPA will oversee all aspects of the project; however, due to its limited staff resources as a member supported organization, it will supervise consultants to undertake most of the tasks outlined in the full Project Management Plan (PMP).

PROJECT OUTLINE

Task 1.0 Advancing Cyber Resiliency and Security Assessments

To better understand the public power community and identify unique challenges faced by utility managers, APPA will conduct a survey and baseline assessment to define and categorize the specific demographics and capabilities of APPA member groups. The demographic analysis of members will hopefully reveal how best to engage public power in the discussion of cyber risk. We then will develop a cyber security maturity model, based on the current DOE C2M2 model, but reduced and refined to be a useful tool for the average distribution utility. Public power managers can then do a self-assessment to

identify risks at their utility. Once the risks are identified the utility manager can focus their limited resources on areas that will have the most impact in improving their cyber security posture.

To help facilitate the task of advancing cyber resiliency and security assessments, APPA will develop targeted security training, conduct technical workshops, exercises, and/or roundtable discussions, offer facilitated risk assessment sessions, along with facilitated sessions using the new public power maturity model, develop cyber resiliency and security-themed videos and/or presentation materials and evaluate ways to match current cyber security technologies and services to utilities that have the capability and desire to deploy them.

Task 2.0 Onsite Vulnerability Assessments

For those public power utilities that have the capability and the desire for a more in-depth look at the vulnerabilities that exist in their cyber systems, APPA will use a consultant to conduct on-site vulnerability assessments across a variety of demographics identified in Task 1. These assessments are intended to explore the varying conditions and operating realities present throughout different segments of the public power community, and how these unique characteristics affects the maturity and effectiveness of cyber resiliency and security programs. APPA will engage the services of a consultant to develop and conduct these assessments.

Task 3.0 Extend and Integrate Technologies (Task 3 expenditures have a 20% cost share obligation)

APPA will engage a consultant to conduct an evaluation of existing technology and cyber security subscription services, for comparing options that would best serve the public power sector from both a technology and resource standpoint. Based on these findings, further deployment across a broader segment of public power may be pursued. APPA will solicit member cost sharing for these deployments. A user group will be formed to provide feedback on the usefulness and usability of these deployments. The user group will work with a consultant to develop a report evaluating the sustainability of the broader deployment of managed cyber security services, recommendations for enhancements to the technology that would benefit the public power community, and ideas for future research needed to develop the technology.

Evaluate deployment of commercial and pre-commercial devices at utilities with the capability to deploy and manage these devices themselves. APPA will establish a team of technical experts from within its member utilities who will evaluate and begin to deploy commercial and pre-commercial security technologies at public power utilities. To accomplish this, APPA will hire a subject matter expert to manage the team's efforts. The team will analyze emerging technologies and existing commercial offerings to develop a catalogue of solutions that may be useful for deployment at public power utilities. Using the demographic data, along with an understanding of the maturity levels of members, the team may recommend classes of technologies that are appropriate for the maturity level of a public power utility.

For utilities with fewer than 2,000 customers, offered on a first-come, first-served basis, APPA will offer a 3-year subscription to the eReliability tracking service. Though these utilities may only have 2-3 staff on average, it is intended that this effort reach up to 65 utilities. This will help the smallest public power utilities transition from paper reliability records and participate in the APPA/DOE/Lawrence Berkeley National Lab (LBNL) research regarding resiliency and econometric evaluations of resiliency improvements.

APPA staff in coordination with DOE and LBNL staff will develop and implement advanced reliability and resiliency reporting algorithms and research. This research may include econometric measures that help utilities assess customer-specific reliability improvement priorities, including ICE Calculator model integration and enhancement and weather factor-based system distress modeling. The results will be used to create predictive resiliency metrics, including cost estimates associated with outages, which can be used to assess the potential impact of cyber related events.

Task 4.0 Information Sharing

APPA will continue to encourage members to use the E-ISAC information sharing portal as the preferred forum for industry threat and situational awareness information. Through this program APPA will evaluate information sharing tools and technologies that will improve the information sharing process for the public power community. New information-sharing methodologies may incorporate a variety of technologies to reduce the time burden placed on the reporting entities, while ensuring interconnectivity with public and private partners in public safety, security, and community resiliency. APPA evaluate programs and reach out to members for recommendations on secure platforms that will assist public power to share threat and cyber incidences easily.

Due to limited resources, many utilities are unable to efficiently process the deluge of threat alerts, including how to identify and respond to the data that is important to them. Once unique demographic groups are identified under Task 1, APPA will hire a consultant to explore a risk-based framework for determining priority levels for the dissemination of secure messages and notifications for public power. The consultant may develop recommendations for E-ISAC on how to categorize, assess, disclose, and disseminate secure threat information that is useful and understandable for public power utilities. The consultant will develop a report that addresses key findings.

APPA will develop a security information engagement plan for public power utility managers for their use to inform their colleagues, city officials and other key stakeholders. The focus of this engagement plan will be to improve understanding of the unique needs of the public power utility especially related to grid security, segmented access rights, and specialized employee training or on-boarding. This will also make it easier for utility managers to communicate with organizational leadership, state, and federal partners when there are credible threats and concerns. APPA will hire a consultant to conduct the engagement and develop content for members to use.

FUNDING

The Consolidated Appropriations Act, 2016, provides $206 million for Department of Energy's (DOE's) Office of Electricity Delivery and Energy Reliability. (OEDER) In this appropriation "not less than $5,000,000 to develop cyber and cyber-physical solutions for advanced control concepts for distribution and municipal utility companies." APPA has partnered with the DOE and has signed a Cooperative Agreement for up to $2.5 million[1] per year for 3 years[2]. With this funding, APPA will accelerate its efforts to help its members understand and implement resiliency, cyber security and cyber-physical solutions, including refining and improving the adoption of advanced control concepts where applicable.

[1] The National Rural Electric Cooperative Association (NRECA) signed a cooperative agreement for the other half of the $5 Million appropriation.

[2] APPA's award was for up to $7.5 million over 3 years; July 1, 2016 – June 30, 2019. Year 1 is totally funded but years 2 and 3 are dependent on Congressional appropriations.