AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

Improving the Cyber Resiliency and Security Posture of Public Power

Final Report

PREPARED BY:
Nathan Mitchell – Principal Investigator
Senior Director, Cyber and Physical Security Services
American Public Power Association
202-467-2925
NMitchell@PublicPower.org

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

Executive Summary

The key objective of Improving the Cyber Resiliency and Security Posture of Public Power (Project) was to develop a culture of cyber resiliency and security within the public power community. The relative smaller size and unique structure of community-owned electric utilities can sometimes present challenges in immediate recognition of threats and the escalation of potential incidents. The Project offered targeted education, coordination, capability building, and resources to help the public power community better understand, install, and implement cyber and physical resiliency and security systems.

The American Public Power Association (APPA) accelerated efforts to develop resources for and with the public power community to understand and implement resiliency, cybersecurity and cyber-physical solutions, including refining and improving the adoption of advanced control concepts. The Project consisted of four major multi-pronged tasks which included: 1) Advance cyber resiliency and security assessments; 2) Conduct, evaluate, and use the results of onsite vulnerability assessments; 3) Research, evaluate, deploy, and integrate both commercial and pre-commercial security technologies; and 4) Research, evaluate, and implement information sharing mechanisms.

1) Advance cyber resiliency and security assessments

Self-Assessments

APPA created the Cybersecurity Scorecard (Scorecard) to help small and medium public power utilities understand where their cybersecurity practices stand. The Scorecard is an easy-to-use self-assessment that simplifies the Department of Energy Cybersecurity Capability Maturity Model (C2M2) for public power utilities to get started on improving cybersecurity. The Scorecard created an easy entry point into assessing foundational utility practices and in gradually introducing utilities to terminology and more complex solutions over time. This approach allowed utilities to get a baseline picture of which practices they are doing well and where they should address key gaps. The Scorecard was a jumping off point for utilities to transition to the full C2M2 assessment and provided a foundation for other program activities.

More than 350 public power utilities completed at least one Scorecard assessment during the Project.

Training and Guidance

Scorecard assessments showed common knowledge gaps regarding cybersecurity within the public power community. APPA created public power utility specific training and guidance to help fill these gaps, including:

- Cybersecurity 101 and 201 training
- CAPP Flex Cybersecurity Exercises
- Cybersecurity awareness videos
- Managed Cybersecurity Service Providers for Electric Utilities
- Public Power Cybersecurity Roadmap
- Public Power Joint Action Agency Cybersecurity Services Plan
- Public Power Cyber Incident Response Playbook
- Cybersecurity Information Engagement Plan

More than 225 individuals participated in training courses offered. In addition, the guidance documents were distributed to participants at key industry events and downloaded from www.PublicPower.org. Through the course of the Project, resources developed received more than 1,860 downloads.

2) Conduct, evaluate, and use the results of onsite vulnerability assessments

Onsite Assessments

To take a deep dive into public power cybersecurity programs, some utilities engaged a third-party consultant to conduct an independent evaluation of their policies, procedures and cybersecurity controls. The evaluations gave utilities professional advice on strengthening cyber and physical defenses and insight into how to improve controls to mitigate vulnerabilities. Each utility received a full report on key findings and recommendations from the onsite assessments.

Through this Project, 21 public power utilities received detailed onsite assessments. Each year of this task, APPA also created a summary report of the common vulnerabilities discovered, which informed resource development and Project activities.

Network Monitoring Tool Suite

Public power utilities with more mature cybersecurity programs often have in-house capability to implement more advanced tools to defend their networks. For these utilities, APPA developed a tool suite of free online resources that utilities could use without hiring a consultant.

3) Research, evaluate, deploy, and integrate both commercial and pre-commercial security technologies

Deploy Cybersecurity Technologies

Some public power utilities do not have the in-house capability to monitor for and alert on malicious activity on their network. These utilities often seek a Managed Security Service Provider (MSSP) to provide constant monitoring and to advise the utility on response and recovery from an incident.

APPA deployed IT monitoring devices and services at 43 public power utilities.

Integrate ICE Calculator

A key part of understanding cyber risk is being able to quantify the potential cost of a cyber incident or attack. Not just the lost revenue to the utility, but the economic effects on the local community served by the utility. APPA integrated the Lawrence Berkeley National Laboratory's Incident Cost Estimator (ICE) calculator, which can be used to estimate the cost of a Ukraine-type cyber-attack scenario, into eReliability Tracker, APPA's proprietary reliability tracking software.

The eReliability Tracker is in use at more than 500 utilities.

Track Cyber Assets

An early indicator from the baseline assessments showed that public power utilities needed a way to track and assess their cyber assets. APPA developed a GIS-based Cyber Asset Tracker software for cataloging cyber assets and comparing the asset list to current vulnerability lists. At the conclusion of the Project, the software is in an alpha testing phase.

4) Research, evaluate, and implement information sharing mechanisms

Security Data Sharing

The myriad of threat and intelligence feeds can easily overwhelm any utility, and digesting all of this information can be particularly burdensome for public power utilities that have small staffs or limited resources. APPA engaged trained cyber analysts to digest threat data into a weekly report of actionable information.

The Weekly Situation Report has been distributed to more than 500 public power utility personnel. This service will continue outside of the Project to keep APPA members apprised of important security information.

Shared Cyber Analyst Program

Some public power utilities identified a need for onsite cybersecurity and IT services. APPA piloted a Shared Cyber Analyst Program in collaboration with a joint action agency (JAA) to provide small entities with additional local support in digesting threat information, offering training, conducting mitigation activities, and providing other cybersecurity services. The JAA will continue to provide this program as a service to its membership.

Cybersecurity Summit

Public power utility security personnel wanted a forum to network with peers and share lessons learned. APPA planned and delivered three national and three regional Cybersecurity Summits that offered this forum with a specific public power focus on cybersecurity practices and trends.

More than 440 public power leaders and staff attended these summits.

Project Conclusion

Developing a culture of cybersecurity at public power utilities requires: an easy entry point into assessing foundational utility cybersecurity practices, resources and guidance that is written and presented for the layperson, tools and services to assess cyber security risk and monitor malicious cyber activity, and trusted forums to exchange current threats and mitigation practices. The Project was successful in developing these resources for public power utilities and moving the industry forward on cybersecurity practices. These tools and resources will continue to guide public power utilities in maturing their cybersecurity programs and in readying them to take the next step to install and implement cyber and physical resiliency and security systems.

Project Outcomes

Task 1.0 Advancing Cyber Resiliency and Security Assessments

The Recipient will utilize the National Institute of Standards and Technology (NIST) Cyber Security Framework, DOE Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) tool, or equivalent as a baseline, to work with its membership to conduct assessments and develop a database to support ongoing benchmarking. The assessments will result in the development of a framework, guidelines, educational material, and the advancement of resiliency and security tools for public power providers.

Self-Assessments

APPA created the Cybersecurity Scorecard (Scorecard) to help small and medium public power utilities determine where their cybersecurity practices stand. The Scorecard is an easy-to-use self-assessment that simplifies the Department of Energy Cybersecurity Capability Maturity Model (C2M2) for public power utilities to get started on improving cybersecurity. The Scorecard created an easy entry point into assessing foundational utility practices and in gradually introducing utilities to terminology and more complex solutions over time. This approach allowed utilities to get a baseline picture of which practices they are doing well and where they should address key gaps. The Scorecard was a jumping off point for utilities to transition to the full C2M2 assessment and provided a foundation for other program activities.

More than 350 public power utilities completed at least one Scorecard assessment during the Project.

Task 1.1: Conduct baseline assessments

The DOE C2M2 tool was selected as the preferred method to develop a baseline assessment. With input from a statistically significant sample of public power utilities, APPA analyzed existing cyber and physical resiliency and security capabilities to define the current resiliency landscape in public power.

Task 1.1, Year 1: The Public Power Cybersecurity Scorecard Pilot Benchmark Report includes data on security and resilience capabilities, risk, and/or demographics of public power utilities. We surveyed public power utilities and facilitated workshops to gain an understanding of the starting point for the project.

Year 1 results from Task 1.1

- Developed online baseline assessment survey.
- Conducted five C2M2 workshops.
- Captured input from 180 public power utilities using the baseline assessment.

Year 1 key findings from Task 1.1

- Only 55% of public power utilities surveyed had a utility-wide cybersecurity program.
- 50% did not have a cybersecurity risk management document.
- 65% of public power utilities surveyed requested more training and information on creating a cybersecurity program.

Task 1.1, Year 2: Further benchmarking was needed to inform the development of tools and guidance documents. The initial Cybersecurity Scorecard (Scorecard) created in Task 1.3 was piloted in Year 2 and helped to enhance the data sets for benchmarking public power.

Year 2 results from Task 1.1

- Continued use of online Scorecard by 141 people.
- Captured input from 95 public power utilities using the Scorecard.

Year 2 key findings from Task 1.1

- Uniform messaging and marketing can drive increased use of the Public Power Cybersecurity Scorecard.
- Users have questions regarding terminology and could benefit from outreach to a user group to address these questions.
- Utilities could benefit from additional policy templates for threat and vulnerability management.

Read more in the Public Power Cybersecurity Scorecard 2018 Annual Report

Task 1.1, Year 3: The Cybersecurity Scorecard is in full use. To drive engagement, APPA facilitated in person presentations, three regional summits and conducted outreach at all APPA conferences. APPA and Axio Global worked with public power utilities to improve dashboard features, conduct informational sessions, collect feedback on platform usability, and provide support to Scorecard users. Tools that allow for analysis of aggregated and anonymized data is incorporated within the platform. A no cost time extension was signed between APPA and DOE to continue the program through September 30, 2020.

Year 3 results from Task 1.1

- The online Scorecard platform use has increased to 520 people representing 287 public power utilities.

Year 3 key findings from Task 1.1

- Public power utilities continue to excel at Identity and Access Management (IAM) and overall Risk Management (RM) domains.
- Public power utilities continue to have gaps and request more information on the Information Sharing and Communications (ISC) and Supply Chain and External Dependencies Management (EDM) domains.
- APPA continues to provide more outreach to join the E-ISAC for information sharing and developing guidance on supply chain vulnerabilities.

Read more in the Public Power Cybersecurity Scorecard 2019 Annual Report

Task 1.1, Year 4: No funds were allocated for a baseline assessment in Year 4.

Year 4 results from Task 1.1

- No further analysis of baseline data was needed.
- Outreach efforts were focused on a few geographic areas to increase the number of participants in the program with 349 utilities completing 742 total assessments and 80 utilities utilized the full C2M2 assessment.
- All comparison data is integrated into the Scorecard platform.

Year 4 key findings from Task 1.1

- Large utilities are more likely to perform multiple assessments
- Outreach plays a significant role in acceptance and adoption of the Scorecard

Read more in the Public Power Cybersecurity Scorecard 2020 Update

Task 1.2: Define and categorize the specific demographics and capabilities of APPA member groups

APPA used a consultant with expertise in analyzing demographic data to compile the results of the baseline assessments in Task 1.1. The contractor identified ways to categorize public power utilities based on security and resilience capabilities, risk, and/or size. These categories informed the development of the Scorecard, accounting for the unique posture and capabilities of public power utilities.

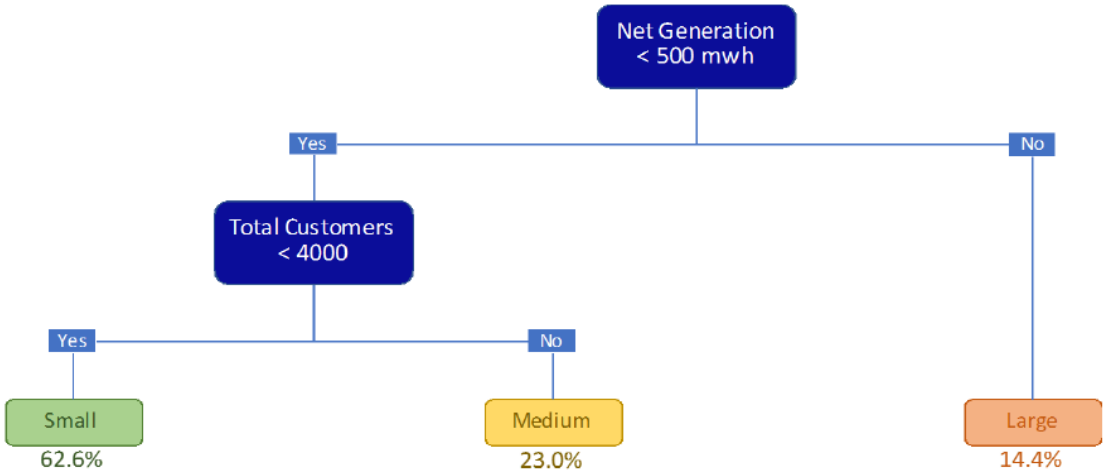
Year 1: APPA compiled the results of the baseline assessments generated in Task 1.1. APPA also analyzed the data from the baseline assessments based on security and resilience capabilities, risk, and/or size.

Year 1 results for Task 1.2

- Data from EIA and Platts was analyzed to find that public power utilities can be segregated into three distinct groupings. 290 Large (Net Generation over 550 MWh), 461 Medium (Net generation less than 550 MWh and more than 4000 customers) 1,255 Small (less than 4000 customers).
- Data compilation was completed from the 180 public power utilities that took the baseline assessment.
- Data was analyzed to assess security capabilities and needs of public power utilities.

Year 1 key findings from Task 1.2

- Additional data is needed to assess small to medium public power utilities' cybersecurity capabilities and needs.
- The assumption was made that a majority of the medium and large public power utilities would have industrial control systems (ICS) in use and a majority of the small public power utilities would not have ICS.
- ***Task 1.2 completed in Year 1 – no further action needed***



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

Task 1.3: Develop Public Power Resilience and Security Maturity Model

Following the baseline resiliency assessments and demographic analysis, the team used the DOE C2M2 to do an initial facilitated assessment with volunteer public power organizations. Anonymized data from these assessments informed the development of a tailored C2M2 that addresses the size, function, capability and scope of distribution systems for public power organizations. In order to assist organizations with determining how to best identify cyber risk and plan for appropriate cybersecurity investment, it is important for the project to take the existing C2M2 and develop the tailored maturity model to be delivered as the Cybersecurity Scorecard. This Scorecard will identify the foundational maturity levels that a public power organization should reach for each of the associated cybersecurity controls in the ten ES-C2M2 domains. Using this Scorecard, organizations can begin to measure their security posture and identify areas for improvement. The Scorecard enabled public power utilities to understand the characteristics of mature cyber and physical resiliency and security programs, processes, and tools, and helped them enhance their programs based on their organizational structure and risk profile.

Task 1.3, Year 1: Based on the results of the Year 1 Baseline Assessment, APPA developed a pilot of a Scorecard for public power utilities.

Year 1 results for Task 1.3

- Conducted five in person facilitated C2M2 workshops, 124 participants representing 41 utilities to establish a baseline;
- Development of the Project Thesis and Roadmap
- The Public Power Resilience and Security Maturity Model was developed;
- A user's group was formed to pilot the Maturity Model and provide feedback; and
- An initial assessment of the Maturity Model was completed.

Year 1 key findings from Task 1.3

- The public power utilities that participated in the C2M2 workshops found real vulnerabilities and consequences that they might not have understood or appreciated prior to the session.
- The Maturity Model is a useful framework for public power utilities to understand the characteristics of mature cyber and physical resiliency and security programs, processes, and tools.
- The Maturity Model will help public power utilities to enhance their cybersecurity programs based on their organizational structure and risk profile.

Task 1.3, Year 2: Based on the results of Year 1 efforts, the Public Power Cybersecurity Scorecard was officially launched. It focuses on the MIL 1 practices from The C2M2 and is written specifically for public power utilities.

Year 2 results for Task 1.3

- A public power utility users group was established.
- The users group provided feedback on the Scorecard and conducted a pilot to ascertain public power understanding of the Scorecard, ease-of-use and gaps.
- The Scorecard was launched at APPA's National Conference in June 2018.
- Engagement plans, including email communications, roadshow schedules, conference planning, a marketing slick-sheet and banners, were developed in preparation for go-live and post go-live user engagement of the Scorecard.
- Established a virtual discussion board for Scorecard users group and an informative webinar series aligned to the Scorecard domains as part of the engagement plan.
- Scorecard statistics:
  - 95 public power utilities filled out assessments
  - 141 unique users
  - 136 Scorecard assessments completed, including 55 full C2M2 assessments started or completed.

The Scorecard was finalized and made available to public power utilities as a free online resource.

Year 2 key findings from Task 1.3

- The Scorecard has proven to be a very useful tool for public power utilities to understand the characteristics of mature cyber and physical resiliency and security programs, processes, and tools;
- The Scorecard continues to help public power utilities enhance their cybersecurity programs based on their organizational structure and risk profile;
- The results of the Scorecard from those utilities which have used it indicate that the early adopters are moving past the Scorecard fundamentals and on to a full C2M2 assessment; and

Task 1.3, Year 3: Based on the results of Year 2 efforts, APPA continued to conduct outreach to public power utilities. Facilitated in-person sessions and presentations at cyber summits and APPA national conferences.

Year 3 results for Task 1.3

- 3 regional summits focused on the foundational practices of the Scorecard
- 1 national Cybersecurity Summit highlighted the Scorecard and Roadmap compatibility

- The target was to reach 400 utilities by the end of the calendar year. By the end of Year 3, 328 utilities completed at least one assessment, and many completed more than one assessment, resulting in 688 total assessments.
- Based on trends in Scorecard use after the conclusion of a workshop, a minimum of eight regional workshops in 2020 would be required to meet the desired target.
- Even though the 2019 goal of 400 was not reached, the 328 signups show the capability of the program to reach the target audience and deliver resources to geographically diverse utilities.

Year 3 key findings from Task 1.3

- The Scorecard provides resources and information to utilities on cybersecurity program development, risk management, and supply chain management.
- Public power utilities need guidance on cybersecurity workforce management, including recruitment and training insights as well as guidance on how to leverage managed security providers.
- There's a need for templates for incident response documents, tabletop exercises, and training.
- Pulling insights from onsite vulnerability assessments will allow for examination of best practices in logging and monitoring activities.
- Public power utilities need training on cybersecurity program and policy development, incident response, risk assessments, cybersecurity awareness, and information sharing.

Task 1.3, Year 4: Based on the results of Year 3 efforts, APPA continued to conduct outreach to public power utilities. However, due to the Covid-19 pandemic, all in-person meetings were canceled.

Year 4 results for Task 1.3

- 2 in-person facilitated sessions were conducted prior to Covid-19 travel restrictions
- 1 virtual facilitated session was conducted
- The Cybersecurity Scorecard was converted to a paid service for public power utilities with further analysis of aggregated and anonymized data within the platform.

Year 4 key findings from Task 1.3

- The restrictions on travel and focus on Covid-19 response by utilities had a significant impact on getting new utility participants to sign up.
- 505 completed Scorecard assessments
- 170 completed full C2M2 evaluations
- 748 total assessments
- 353 participating utilities
- 687 total users

Self-Assessment Conclusion

Public power utilities found the foundational practices of the Scorecard useful in conducting a self-assessment of their cybersecurity program. A significant number of public power utilities have moved on to conduct full C2M2 self-assessments and are utilizing more tools within the platform to continue to improve their cybersecurity program. In October 2020, APPA and Axio Global entered into an agreement to provide public power utilities access to the APPA-branded

Axio platform as a commercial offering. This agreement will help users retain their historical assessments and continue with access to the full suite of services provided by Axio, which include C2M2 assessments. The platform is now called Axio 360 for Public Power.

Training and Guidance
Scorecard assessments showed common knowledge gaps regarding cybersecurity within the public power community. APPA created public power utility specific training and guidance to help fill these gaps, including:

- Cybersecurity 101 and 201 training courses (Task 1.4)
- CAPP Flex Cybersecurity Exercises (Task 1.5)
- Cybersecurity awareness videos (Task 1.6)
- Managed Cybersecurity Service Providers for Electric Utilities (Task 1.7)
- Public Power Cybersecurity Roadmap (Task 1.8)
- Public Power Joint Action Agency Cybersecurity Services Plan (Task 1.8)
- Public Power Cyber Incident Response Playbook (Task 1.10)
- Security Information Engagement Plan for Public Power (Task 4.4)

More than 225 individuals participated in training courses offered. In addition, the guidance documents were distributed to participants at key industry events and downloaded from www.PublicPower.org. Through the course of the Project, resources developed received more than 1,862 downloads.

Task 1.4: Develop targeted training opportunities

APPA conducted training related to the unique cyber and physical resiliency and security posture of public power. Several of these training sessions were conducted in tandem with conferences and others were offered via webinar and online training modules. APPA utilized professional trainers with expertise in the cyber, resiliency and security areas identified as priority for members to address. At the conclusion of these efforts, APPA developed a report that evaluated the courses and instructors and suggested an efficient direction for future training offerings.

Task 1.4, Year 1: Training is essential to ensuring the public power workforce understands the security landscape and uses the cybersecurity tools to further enhance their cybersecurity maturity level. APPA conducted several training sessions identified as gaps in the baseline assessment in Task 1.1 and in line with the foundational practices of the Scorecard developed in Task 1.3.

Year 1 results from Task 1.4

- During Year 1, several training sessions were planned, conducted and feedback was received.
- APPA collaborated with the SANS Institute, EnergySec, AESI, and N-Dimension to provide free or reduced cost training for public power utilities.

Year 1 key findings from Task 1.4

- Training session participants found real vulnerabilities and consequences that they may not have understood or appreciated prior to the session.

- Training session participants indicated that they struggle to achieve management buy-in for cybersecurity controls, as senior management does not see an imminent threat to the utility.

Task 1.4, Year 2: APPA continued to sponsor multiple training sessions and lectures related to the unique cyber and physical resiliency and security issues of public power utilities. APPA continued its collaboration with the SANS Institute, EnergySec, AESI, and N-Dimension to provide reduced cost training for public power utilities.

Year 2 results from Task 1.4

- The training catalog was completed and distributed to joint action agencies (JAAs) and state and local agencies to identify interest in hosting training and scheduling dates.
- 12 training sessions and lectures were conducted under the Cooperative Agreement with 129 attendees; another three sessions conducted under APPA's Academy training program with an additional 70 attendees.
- Of the 199 attendees, 131 provided training session evaluations. The evaluations provide insight for future training enhancements.
- APPA entered into a collaborative arrangement with Kansas Power Pool (KPP) and Custom Internet Services (CIS) to develop and deliver new cybersecurity training content based upon the foundational practices of the Scorecard and with input from KPP constituents.

Year 2 key findings from Task 1.4

- Training session participants liked the hands-on aspect of the training. Those new to the topic commented that there was a large amount of material (sometimes overwhelming) presented.
- Public power utilities want training specific to *their utility's* needs.
- Public power utilities want ongoing training on all aspects of managing a cybersecurity program. Suggested topics include:
    - How IT/network/systems administration and engineers can protect their systems from cyber attacks.
    - Policies and best practices.
    - How to train users.
    - How utilities implement firewalls and edge devices.
- Initial analysis of the training feedback was aligned to a newly developed logic model. The elements of the logic model's estimated outcomes and impacts include:
    - Learning outcomes such as increasing awareness, commitment to action, and alignment with the Scorecard.
    - Behavioral outcomes such as true executive motivation to action as champion or by conducting process changes or purchasing new technology. This should extend to non-participant behavioral changes (utility staff members who did not attend training).
    - Direct cybersecurity impacts such as changes in the organization's cybersecurity strategy, policy, procedures, culture, or practices and improvements in cyber maturity. Utilities can expect improved maturity, improved cybersecurity threat detection, and improved responses to threats.
    - Company/organizational impacts including positive impact on bottom line, brand/image with customers, and enterprise risk.
    - Societal impacts such as improved infrastructure security, increased technology

adoption and innovation, and increased grid/system reliability.
  - Most utility participants who completed the training session evaluations indicated that they *gained specific knowledge* in the following topic areas:
    - Establishing and operating cybersecurity risk management.
    - Managing cybersecurity threats and vulnerabilities.
  - Utility participants who completed the training session evaluations *gained at least general knowledge* in the following topic areas:
    - Management and inventory of assets.
    - Cybersecurity training and workforce management.
- Public power utilities found that the Ukraine incident has been discussed in cybersecurity training over and over again.
- The CyberStrike hands-on demonstration of the Ukraine scenario was a good example of collaboration between APPA and DOE national labs in a training environment.

Task 1.4, Year 3: In Year 3 members requested to focus on OT-specific cybersecurity training. Therefore, APPA developed a scope of work and hired a consultant to develop and provide this training.

Year 3 results from Task 1.4

- APPA hired Dragos Inc. to develop an OT specific cybersecurity training for public power utilities.

Year 3 key findings from Task 1.4

- 33 public power utilities participated in the OT Cybersecurity Training.
- The training session received positive feedback.
- The OT Cybersecurity Training models have been incorporated into the APPA Academy for virtual and in-person training.

Task 1.4 Conclusion

Summary from CEDS Training Program Results Summary (final report):

To improve the level of cybersecurity expertise among public power utilities, the American Public Power Association established a catalog of training courses offered to member utilities. Throughout 2017 and 2018, municipalities, utilities, and joint action agencies scheduled training sessions from the course catalog. During the program, training sessions saw broad participation from a cross-section of the public power sector including both technical and executive leadership roles. In total, 256 participants attended 19 sessions in 17 locations across the country.

At each session, participants were asked to complete a course evaluation to capture feedback and provide an immediate measure of the effectiveness of the training across several metrics. The evaluation form collected consistent data across training sessions, courses, and providers, no matter the intended audience. Metrics included the impact of the course on specific cybersecurity topics, the actions participants would take, and the general feedback on the instruction offered. The evaluation form also provided an opportunity for participants to offer recommendations for improvements to the class or ideas for future topics. The feedback captured in the evaluation forms demonstrated many positive outcomes from the training services including:

- Increased knowledge and likelihood of taking actions to improve cybersecurity

- Increased sense of urgency and ability to communicate cybersecurity issues
- Provided knowledge to overcome barriers or identified remaining barriers
- Overwhelmingly positive assessment of instructors and trainings

The data collected and comments submitted through the evaluation forms suggest several recommendations:

Continue to offer training to the public power community. More than 90% of evaluations said trainees would recommend courses to colleagues or would take another training. There is likely still demand for this type of training so it should be continued.

Continue to be clear on prerequisites and learning expectations for courses. IT/OT overview training is useful for the right audience—it is a good primer for managers and those IT/security staff new to the utility space but less useful for knowledgeable security subject matter experts (SMEs).

Continue to offer quality introductory/overview courses from a variety of vendors. Although several deeper-dive cybersecurity topics were offered through the course catalog, few members selected these courses. This could be an indication of the relative cyber-immaturity of the industry or could be an indication that intermediate or expert knowledge is embedded in a small number of staff (not enough to populate a group training session).

Offer individual training for specific cybersecurity topics but advertise these to the right market. Those that took SANS training appreciated the focused topics available and methods for training.

Provide in-person training as close to work sites as possible and encourage group discussion and exercises. In-person training tended to be preferred over web-based training; evaluations showed the least positive support for convenience of course location. Even the web-based training (other than SANS) saw groups of individuals gathered together to take the training. Trainees value group discussion and Q&A.

Training programs have been incorporated into the APPA meetings department offerings and will continue to be offered in-person, at conferences and in virtual format.

Task 1.5: Conduct technical workshops, exercises, and/or roundtable discussions

APPA facilitated technical workshops, exercises, and roundtable discussions to challenge assumptions and test models developed in this Project. These exercises were intended to reach a wide variety of audiences and perspectives to gather additional insight into the characteristics and processes unique to public power utilities.

Task 1.5, Year 1: A cyber exercise expert was hired to plan and conduct in person Cyber and Physical Preparedness (CAPP)-Flex exercises.

Year 1 results for Task 1.5

- 14 tabletop exercises conducted.
- Tabletop exercise results aggregated and submitted to DOE.

Year 1 key findings from Task 1.5

- Many public power utilities are not familiar with E-ISAC.

- There is a need for cyber threat identification and incident response training.
- There is limited availability and use of planning and response documents and procedures specific to cybersecurity threats and incidents.
- Large amounts of messages from intelligence sources have resulted in alarm fatigue, ultimately diminishing the effectiveness of the information sharing program.
- ***Year 1 effort completed – no further action needed.***

Note: the tabletop exercises under Task 1.5 in Year 2 were rolled into Task 1.10 - Incident Response Playbook development and exercising.

Task 1.5 Conclusion

An after-action report was published for official use only, but key findings and recommendations are as follows.

Key Findings

Public power utilities need cybersecurity training tools and guidance.

Many indicated that there is generally low awareness of cybersecurity risks at both the organizational and individual levels. Participants expressed interest in receiving additional tools, guidance, and training in support of their cybersecurity programs and business continuity plans and additional education on threat assessments and identifying vulnerabilities.

Future exercises should be tailored to the type, size, and general capabilities of the audience. Scenarios examining ransomware, attempts to gain access to customer employee personal information, etc., or other attacks impacting email, phone, and file systems should be used (in addition to or in place of the Ukraine scenario) to craft more relevant exercise materials.

Exercises should be scaled to encouraged active participation from attendees, via breakout discussions.

Public power utilities need guidance on information sharing and media response.

Many had concerns with communicating and sharing information on threats or possible attacks with individuals and entities outside of their own organization, including the media, local government stakeholders, as well as local law enforcement and federal agencies.

Participants expressed an interest in receiving guidance on how to address cybersecurity issues to make staff and co-workers more aware of cyber risks.

There is a need for APPA to provide guidance outreach, training, and potentially technical support regarding the appropriate sharing of information and use of the E-ISAC.

Recommendations

Deploying technologies

One technology-related issue that was discussed multiple times was real-time information sharing via portals, email notification, message boards, or other means specific to utilities. APPA might consider providing an overview of available technologies that members could employ within their organizations. APPA and JAAs should also advise all members to participate in E-ISAC, including provision of any support necessary in walking them through the process. APPA should also evaluate the development of a secure member communication and document

sharing platform.

Developing tools

APPA should consider offering members onsite or remote evaluations, gap assessments, or audits of existing cyber preparedness and response plans and programs. This could include guidance regarding when a threat or incident becomes reportable and Creating a mutual aid framework for cyber responses. APPA should develop media planning tools that can be used by members to prepare for various cyber incidents, including prewritten scripts.

Writing and disseminating educational resources

APPA might develop and deploy educational curricula, awareness campaigns, workshops, videos, and toolkits relevant to public power utilities of various sizes, types, and cybersecurity program maturity.

Updating guides

APPA should develop or refine strategic plans, industry best practice guidelines, reference materials and/or operations framework to cultivate a culture of resiliency and security within the public power community. APPA should expand on the "Procurement Strategies and Third-Party Management" section within the APPA Cyber Security Essentials document.

Conducting exercises and training

APPA should continue conducting seminars, workshops, and tabletop exercises with members to explore cyber and physical threats, management of grid reliability, collection and sharing of best practices. Exercises and workshops should continue to be held at regional meetings. Training and exercises should target varied audiences, including departments and positions within the utility, city IT departments, mayor's offices and city councils, JAAs, and others. Advanced exercises should be considered that include realistic scenarios associated with cyber attacks. APPA should continue to offer regional tabletop exercises specifically geared towards JAA officials and their members.

Undertaking outreach efforts

APPA should continue to conduct outreach activities to JAAs and utility members directly to make them aware of the resources currently available to them and resources that result from these exercises. APPA should continue to promote information sharing about known events and risks through the E-ISAC, while additionally providing membership with actionable information and best practices for responding to these types of events in the future.

Task 1.6: Develop cyber resiliency and security-themed videos and/or presentation materials

Public power utilities needed materials to educate first responders, city officials, and other stakeholders in their communities on cybersecurity issues related to the electrical system.

Task 1.6, Year 1: A subject matter expert was engaged to oversee this task, select a production company, and work with APPA on content and audience selection.

Year 1 results for Task 1.6

- Four videos were developed covering the following subjects: 1.) Cooperative Agreement overview; 2.) Cybersecurity risk assessment; 3.) Cybersecurity incident response; and 4.) Cybersecurity information sharing in an effort to help communicate complex subjects to potentially uninformed stakeholders.

Year 1 key findings from Task 1.6

- Most public power utilities have few, if any, educational materials for stakeholders; and
- Many public power utilities have expressed a need for these educational materials and will utilize the videos whenever possible to educate local law enforcement, first responders, municipal government officials and other key stakeholders.

Task 1.6, Year 2: APPA completed the cybersecurity themed videos initially identified in budget Year 1.

Year 2 results from Task 1.6

- All four videos were posted and made available to utilities for download from APPA's Cybersecurity webpage (https://www.publicpower.org/topic/cybersecurity) and YouTube channel.
- The Cybersecurity 101 video has had 636 views on APPA's YouTube channel as of December 15, 2020.
- The Introduction to Improving the Cyber Resiliency and Security Posture of Public Power (CEDS) video has had 730 views on APPA's YouTube channel as of December 15, 2020.
- The Cybersecurity Risk Management Process for Public Power Utilities video has had 323 views on APPA's YouTube channel as of December 15, 2020.
- The Information Sharing video has had 151 views on APPA's YouTube channel as of December 15, 2020.
- Previously completed videos were updated to include closed captioning to ensure the videos are accessible to a greater community of viewers.
- ***Year 2 effort completed – no further videos produced.***

Task 1.6 Conclusion

The videos provided a quick and simple way to communicate the actions needed to develop a culture of cybersecurity at public power utilities. They were useful in helping to explain a complex topic in a short, visual format and were well received.

Task 1.7: Explore standardized procurement mechanisms

APPA conducted an initial analysis of current cyber and physical security and resiliency technologies to match those technologies to classes of public power utilities with the capability to implement these technologies. Based on the results of the analysis, APPA developed standardized procurement mechanisms that can be used by small public power utilities. A user guide was developed as a deliverable.

Task 1.7, Year 1: Analysis of managed security service providers (MSSPs) was conducted in Year 1, which resulted in the development of a draft Managed Cybersecurity Service Providers for Electric Utilities Technologies Guide (Technologies Guide). The Technologies Guide was designed to align the services and capabilities of the providers with public power utility needs and to provide public power utilities with a concise resource document to assist in procurement decision making.

Year 1 results from Task 1.7

- 48 MSSPs were evaluated and six MSSPs were identified as being good potential

vendors for public power utilities.
- A users group was established to evaluate the MSSPs.
- A user guide of current cybersecurity MSSPs was developed.

Year 1 key findings from Task 1.7
- Many cybersecurity providers serve the utility/electricity sectors and have specific offerings for small business, matching the needs of public power utilities identified by APPA.
- The largest number of companies identified focus their services on managed security monitoring, penetration testing and vulnerability measurements.
- Though cybersecurity MSSPs services are globally available, numerous providers focus on the North American market, thereby ensuring that public power utilities have access to a cybersecurity solution of their choice.
- No single company was identified that offered all the critical and non-critical services required by public power utilities.
- Public power utilities may have to leverage the services of multiple providers in their procurement efforts.

Task 1.7, Year 2: APPA published the Managed Cybersecurity Service Providers for Electric Utilities (Technologies Guide). The Technologies Guide was designed to align the services and capabilities of MSSPs with public power utility needs and to provide public power utilities with a concise resource document to assist in procurement decision making. The Technologies Guide was produced and distributed to 1,400 public power utilities.

Year 2 results from Task 1.7
- The Technologies Guide was offered to all public power utilities.
- As of December 16, 2020, there have been 322 downloads of the Technologies Guide.

Year 2 key findings from Task 1.7
- The Technologies Guide has assisted public power utilities, which have a need for hiring technology vendors, in their procurement decisions.
- One of the identified vendors, N-Dimension, was selected by most public power utility users in Year 1 to provide services. (More information can be found in the Task 3.1 report).
- Task 3.1 is directly related to adoption of technologies identified in the Technologies Guide.
- ***Year 2 effort completed – no further work on the Technology Guide.***

Task 1.7 Conclusion
Public power utilities need guidance on selecting MSSP vendors. Having a resource such as the Technology Guide helps public power utilities identify and categorize vendor service offerings.

Task 1.8: Pilot a Cyber Resiliency and Security Roadmap

New effort in Year 2

APPA developed and piloted a Public Power Cybersecurity Roadmap (Roadmap) that outlines the strategic and tactical steps needed for public power utilities to harden their systems to

achieve cyber resiliency and security infrastructure improvements.

Task 1.8, Year 2: APPA began to develop the Roadmap at the end of Year 2. An advisory group of public power utilities was established to identify the information that should be included in the Roadmap, what steps to take to ensure wide use of the Roadmap, and what training efforts should take place in Year 3.

Year 2 results for Task 1.8

- A contractor was hired at the end of Year 2 to assist APPA in developing the Roadmap.
- Defined an approach for the Roadmap to identify paths to address gaps uncovered as part of the Scorecard assessment.
- Members of an advisory group of public power utilities and joint action agencies were identified.

Year 2 findings for Task 1.8

- Identified key outreach targets for the Roadmap that could serve as change agents for adoption of the Roadmap as it is produced.

Task 1.8, Year 3: APPA worked with the advisory group with the help of a facilitator to develop and finalize the Roadmap.

APPA corresponded with operational and technical personnel at multiple public power utilities to develop a complete view of the many layers of needs, responsibilities, and opportunities facing public power personnel. Team members discussed experiences with cyber threats and incidents as well as experiences collaborating with boards and management to bolster cybersecurity. Team members also discussed accounts of national and international events that offered insight into the scope and nature of cyber threats and countermeasures.

The advisory group identified four stages through which organizations can build and deploy their efforts.

Stage 1: EVALUATE internal and external factors influencing most pressing cybersecurity issues (i.e. complete the Scorecard assessment); locate sponsors and leaders needed to achieve desired changes; generate a list of prioritized opportunities for improving cybersecurity; and consider the organization's strategy and risk tolerance.

Stage 2: FORMULATE a project-based plan to improve cybersecurity; use a risk-based approach to identify two or three promising opportunities for improving cybersecurity; appoint leadership and hire appropriate staff to carry out cybersecurity efforts; and implement managerial, technical, and general staff training.

Stage 3: ACTIVATE the project-based plan by creating ongoing, enforceable policies for all personnel; follow the activities or steps identified in the plan; acquire any necessary new tools or systems then install and test them; institute new policies and procedures needed to support tools and identified improvements to cybersecurity processes; develop a cyber incident response plan (using the Cyber Incident Response Playbook as reference); and design a communications strategy to handle potential cyber incidents.

Stage 4: INTEGRATE practices defined by the plan into the operation of your organization; move new tools or systems into the production environment; ensure any new systems are regularly monitored and regular patches and upgrades are maintained; operationalize and maintain the new process as part of business-as-usual practices. This turns the "new" practices into "standard" practices--making them part of your organization's culture is the final critical

stage in improving cybersecurity and making sure the improvements last. Finally, revisit the Public Power Scorecard to reassess the organization's cybersecurity maturity and to prepare for further evaluation (and return to Stage 1).

Year 3 results for Task 1.8

- The Roadmap is available for download from APPA's website and has been downloaded 533 times through December 15, 2020.
- Public power utilities requested further assistance at the local level, therefore a new team was developed to address cybersecurity from a joint action agency level. The resulting Public Power Joint Action Agency Cybersecurity Services Plan was published in January 2020.

Year 3 findings for Task 1.8

- JAAs have established relationships with utilities and can influence cybersecurity culture and offer services such as technical advice, incident response, security assessments, and training.
- The JAA plan instructs "what" to do, but not "how" to do it; an execution plan addressing leadership and workforce, marketing, financials, and resourcing should be developed.
- Several joint action agencies have developed programs and are piloting paid for services to support their members locally.

Task 1.9: Investigate Cybersecurity Workforce Development Opportunities

New effort in Year 2 (Canceled)

Public power utilities often face difficulties in identifying and recruiting qualified local cyber and physical security candidates due to their location and/or size. Working with universities, community colleges and other educational and training institutions across the nation, APPA should explore the development of opportunities and/or programs that meet the staffing needs of public power utilities and provide for shared resources and training. The purpose of this task is to enhance the security workforce within public power communities and provide opportunities for college students to intern at public power utilities in the cybersecurity field (and eventually become employed in this sector).

Task 1.9, Year 2: Identifying and recruiting public power cybersecurity workforce candidates continues to be a challenge facing public power utilities due to their size and remote locations. However, during Year 2 APPA project team members and stakeholders engaged in hurricane relief efforts resulting in this task being canceled. Efforts were shifted to Task 4.1 to employ shared cyber analysts.

Task 1.10: Develop a Public Power Cyber Incident Response Playbook

New effort in Year 2

Based on findings in the Task 1.5 after-action report, APPA developed a Public Power Cyber Incident Response Playbook to detail the potential roles and responsibilities within a small public power utility in the case of a security incident. In many small utilities, one person has many roles and responsibilities. As such, a step-by-step playbook on what actions to take, who to coordinate with, and other types of response activities will supplement current mutual aid

programs.

Task 1.10, Year 2: APPA hired a contractor to facilitate member outreach, conduct initial research and assist APPA in developing an outline of the Playbook.

Year 2 activities under Task 1.10

- APPA worked with the contractor on the outline for the Playbook.

Year 2 findings from Task 1.10

- Because the contractor was hired and the activities to develop the Playbook were started late in Year 2, activities were carried over into Year 3.

Year 3 activities under Task 1.10

- APPA worked with a consultant, 30 public power utility representatives, and other partners to develop the Playbook.

Year 3 findings from Task 1.10

- The Playbook was well received by members and non-members alike.
- The Playbook is posted on APPA's website for free download and has been downloaded 500 times through September 30, 2020.

Task 1.10 Conclusion

The Playbook provides step-by-step guidance for small to mid-sized public power utilities to help them prepare a cyber incident response plan, prioritize their actions and engage the right people during cyber incident response, and coordinate messaging. The playbook serves three key purposes:

1. Provides guidance to help a utility develop its cyber incident response plan and outline the processes and procedures for detecting, investigating, eradicating, and recovering from a cyber incident.
2. Maps out the industry and government partners that public power utilities can engage during a significant cyber incident to share information, get support for incident analysis and mitigation, and coordinate messaging for incidents that require communication with customers and the public.
3. Outlines the process for requesting cyber mutual aid from utilities across the energy industry for a cyber event that significantly disrupts utility business or operational energy delivery systems and overwhelms in-house cyber resources and expertise.

Cybersecurity managers can use the Playbook as a step-by-step guide to prepare for an incident. Key guidance in the Playbook include:

- Identify the cyber incident response team.
- Identify contacts and response service contracts for cybersecurity service providers and equipment vendors.
- Understand the system and environment.
- Outline incident reporting requirements and timelines.
- Identify the response procedures the Cyber Incident Response Team (CIRT) will take to investigate, contain, eradicate, and recover from a variety of different incidents.
- Develop strategic communication procedures for cyber incidents.

- Define response procedures and responsibilities of the utility's legal team during cyber incident investigation and response.

The Playbook was exercised at APPA's Engineering and Operations Conference in April 2019 to validate the guidance based on a Ukraine type scenario.

Task 1.11: Examine Utility Resiliency using Significant Cyber Incident Scenarios and other Operations Data

New effort in Year 2 using data from Year 1 Task 3.4 results

APPA, in coordination with utilities, universities, DOE, and the National Labs, would research impacts to reliability and resiliency metrics due to various cyber incident scenarios. The purpose of the research was to compare reliability impact data with cyber impact data so that public power utilities will be able to predict outage cost impacts from both a reliability and cybersecurity basis. The research would also provide a foundation for considering cyber asset investments in comparison with other operational investments. Having such comparison data would provide public power utilities with the ability to compare costs to make better investment decisions to ensure the grid remains secure.

Year 2 findings for Task 1.11

- Manipulating utility data streams to cause attacker favorable effects in terms of operations is a threat that was explored on the reliability/resiliency side with the goal of publishing the results of the research in *Data Analytics for Energy, Water, and Environment IEEE Transactions on Engineering Management. Publish date: TBD*

This position paper proposed a new research topic on the data integrity attacks to outage management systems and discussed scenarios of such attacks, including the consequences and means to detect and mitigate the attacks. The proposed research would relate to recent progress in three areas: state estimation, load forecasting, and outage prediction.

Task 1.11 Conclusion

Data integrity attacks to OMS have not been reported in the mainstream media nor formally studied in the academic literature. This research initiates the conversation by pointing out the important role of the OMS in distribution operations, the possibilities of executing a data attack to an OMS, its potential consequences, and several means for detection and mitigation of such data attacks. Further analysis of the data was evaluated and determined to be outside of the scope of the program objectives. Therefore, Task 1.11 was not funded in Year 3.

Task 2.0 Onsite Vulnerability Assessments

The Recipient will conduct assessments and develop case studies of a segment of member entities. The Recipient will evaluate and integrate the processes and technologies available to alert public power utilities of threats and vulnerabilities in their cyber and physical systems and share results to drive continuous improvement.

Onsite Assessments

To take a deep dive into public power cybersecurity programs, some utilities engaged a third-party consultant to conduct an independent evaluation of their policies, procedures, and cybersecurity controls. The evaluations gave utilities professional advice on strengthening cyber and physical defenses and insight into how to improve controls to mitigate vulnerabilities. Each utility received a full report on key findings and recommendations from the onsite assessments.

Through this Project, 21 public power utilities received detailed onsite assessments. Each year of this task, APPA also created a summary report of the common vulnerabilities discovered, which informed resource development and Project activities.

Task 2.1: Conduct assessments, surveys, and field-based fact-finding missions

In Year 1 of the Project, APPA began to conduct initial cyber and physical resiliency and security assessments of public power utilities across a variety of demographics. The assessments continued into Years 2 and 3. These assessments intended to explore the varying conditions and operating realities present throughout different segments of the public power community, and how these unique characteristics affect the maturity and effectiveness of cyber resiliency and security programs. APPA used the services of two consultants to develop and conduct these assessments. The consultants evaluated systems against existing resources including, but not limited to, APPA's Cybersecurity Scorecard, APPA Cybersecurity Essentials Guide, APPA Physical Security Guidebook, and other industry standard guidance.

Task 2.1, Year 1: Onsite assessments are the best protocol to determine security maturity. APPA conducted onsite assessments of public power utilities across a variety of demographics. The assessments intended to identify security capabilities and needs of public power utilities.

Year 1 results from Task 2.1

- 11 onsite assessments conducted.
- Recommended improvement measures were provided to public power utilities which were assessed.

Year 1 key findings from Task 2.1

- Public power utilities had adequate basic security measures in place across physical security infrastructure.
- Security awareness was found to be apparent at the public power utilities visited.
- The use and implementation of certain physical security related systems was not consistent across the public power utilities assessed.
- Limited documented security-specific physical security policies and procedures as well as decentralized physical security responsibilities were found to be consistent opportunities for improvement.

- Common cybersecurity challenges were identified, including; limited documentation of cyber security incident history, limited dedicated physical security of cyber assets, limited access to information technology (IT) staff, no dedicated cyber security staff, and limited documented IT and cyber security policies and procedures.
- Networks which were assessed were typically built to meet evolving needs, resulting in networks that have many unknowns.
- Limited business network segregation among departments was observed.
- Networks assessed typically had a cyber perimeter defense mechanism in place but could benefit from in-depth defense and resilience measures.

Task 2.1, Year 2: APPA was unable conduct onsite assessments due to unexpected circumstances. Although not a cybersecurity event, APPA project team members and stakeholders engaged in hurricane relief during Year 2 resulting in a delay in development of the RFP.

Year 3 results from Task 2.1

- APPA used two subcontractors to conduct onsite assessments. The following sections summarize the findings from each contractor.

Contractor #1 Onsite Assessments

APPA engaged Burns & McDonnell to provide public power utilities with a holistic third-party assessment of the physical security and cybersecurity of their cyber assets. This task consisted of assessing the cybersecurity maturity, policies and procedures, and governance to provide APPA with common risks observed and recommendations for improvement for public power utilities.
Burns & McDonnell's activities are aligned to industry standards such as the National Institute of Standards and Technology (NIST) Standard Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations, the CIS Top 20 Critical Security Controls, and other leading standards. Burns & McDonnell assessed the maturity of member utilities against the Electricity Subsector Cybersecurity Capability Maturity Model (C2M2) utilizing the Public Power Cybersecurity Scorecard.

During this assessment period, the team visited eight (8) public power utilities. These site visits included power generation plants, substations, service centers, operations buildings, city halls, and city data centers. By interviewing key stakeholders of these APPA member utilities and having discussions regarding policies and procedures, Burns & McDonnell received valuable information and insight into how each utility operates. All member utilities visited displayed a dedication to maturing their cybersecurity program, often discussing appropriate strategies at a high level to implement more effective security controls. These discussions also included challenges and perceived opportunities for improvement. .

Some of these high-level observations include:

- Most member utilities did not have a managed cybersecurity program, did not manage or enforce their hardware and software asset inventories, and did not have a way to continuously manage vulnerabilities.
- When member utilities had documentation for policies and procedures, it was solely focused on the North American Electric Reliability Council's critical infrastructure protection (CIP) requirements for bulk electric system (BES) assets. This did not cover

cybersecurity practices such as hardware and software inventory and control, and patch and vulnerability management, or secure configurations. Cyber assets not considered as BES cyber assets (not under purview of NECR CIP) typically did not have any documented cybersecurity policies or procedures and were managed in an ad-hoc manner.

- Member utilities are not following best practices when setting up network infrastructure. Most had a strategy for segregating industrial control system networks, but contradicted this strategy with transient devices or connected ICS networks with external networks through workstations with dual network interface cards.
- While some member utilities have available resources to bolster their information technology infrastructure, these resources are not reflected or shared with the operational technology department.
- Unless OT assets are performing outside of normal bounds from an operations point of view, many member utilities do not have a way to be alerted when there is an intrusion in their system.

Overall, this group of APPA members had more policies and procedures in place, and were generally more mature in their security practices, than public power utilities assessed in previous years. However, most of these practices were solely focused on systems with NERC CIP requirements. An overall recommendation is for these utilities to continue growing their cybersecurity programs in place for their BES cyber assets and to expand their programs to cover all cyber assets. Member utilities should also add other standard practices such as patch and vulnerability management into their cybersecurity programs. The roadmap for cybersecurity improvement never ends, but small steps can be taken to vastly improve an organization's overall security posture. The first milestone a cybersecurity program should try to achieve on this roadmap should be MIL2. MIL1 is seen as a minimum to get a cybersecurity program started and does not represent a secure program.

The findings and recommendations from the onsite assessments, even though they were anonymized, contained sensitive information and is held at the FOUO level and not shared in this report.

Contractor #2 Onsite Assessments

APPA engaged Axio Global to provide onsite assessments of public power utilities to identify security capabilities and needs of utilities across a variety of demographics. APPA contracted with Axio Global to conduct onsite assessments using its Axio360 process to provide a scoring system for addressing gaps and to provide a technology platform to create an improvement roadmap and prioritize closing those gaps.

By leveraging both cybersecurity subject matter experts, including former auditors and security practitioners, and the Axio360 software-as-a-service technology, public power utilities can create action items that tie back to the Public Power Cybersecurity Scorecard, quantify their cyber risk, and more accurately invest and evolve cybersecurity controls across both their information technology and operational technology systems.

Each onsite assessment included a tailored threat briefing, including sector-specific threat analysis and open-source intelligence (OSINT) gathering from subject-matter experts. This ties together with process evaluations and interviews with the utility's leadership, security team, risk management professionals, and engineering staff to ensure an accurate assessment of their cybersecurity program capabilities. Final assessments also included recommended

improvement measures for public power utilities.

The onsite assessments include the following services:

- Cyber program optimization
- Cyber risk quantification
- Insurance analysis and stress test

An initial list of five utilities was identified to participate in the program. Outreach was conducted and two public power utilities accepted and scheduled the facilitated Axio360 engagement. The three other utilities showed interest but could not commit the time and resources necessary to initial document gathering and onsite facilitation. The two assessments were conducted in Florida and Tennessee. Results were delivered to the Florida utility in November 2019 and to the Tennessee utility in February 2020. The projects ended early due to funds being reallocated to other tasks. Therefore, a full analysis of multiple utilities could not be completed. Since only two utilities participated, common findings and recommendations could not be concluded from this small data set.

Lessons Learned

- Having clear objectives and outcomes prior to onsite assessments is necessary.
- Need to articulate the benefit to the organization with internal stakeholders prior to the engagement to get senior leadership buy-in.
- Final report was thorough but overwhelming.
- When final report was delivered it was hard to implement the recommendations without clear linkages to who within the organization was responsible for mitigation.

Task 2.1 Conclusion

Public power utilities found value in the onsite assessments. Having a third-party analysis of their program, policies and procedures and cybersecurity controls gave the utilities validation of the positive activity happening within their programs. However, many of the reports were overwhelming for most small utilities with limited budgets to implement changes and no real roadmap to prioritize efforts.

Task 2.1 Additional Tools

Network Monitoring Tool Suite

Public power utilities with more mature cybersecurity programs often have in-house capability to implement more advanced tools to defend their networks. For these utilities, APPA developed a tool suite of free online resources that utilities could use without hiring a consultant.
APPA contracted with Burns and McDonnell to curate open-source tools that could be used by public power utilities. An initial analysis of available open-source tools was conducted and a Tool Suite Comparison document was developed. The APPA Cybersecurity Tool Suite is a collection of open-source industry software tools created to provide APPA members with insight and visibility into their environment. This visibility provides utility staff the ability to create and execute a targeted, prioritized strategy to remediate vulnerabilities within their networks.

The final Tool Suite was tested and offered for utilities to deploy with help of the third-party developer, Burns and McDonnell. Public power utilities are provided a fully customizable dashboard for visualizing event data with the ability to drill into specific events to gather

additional information. Further details can be gathered using the tool suite's fully automated Hardware/Software Inventory Tool and Vulnerability Scanner.

Task 3.0 Extend and Integrate Technologies

The Recipient will conduct assessments and develop case studies of a segment of member entities. The Recipient will evaluate and integrate the processes and technologies available to alert public power utilities of threats and vulnerabilities in their cyber and physical systems and share results to drive continuous improvement.

Deploy Cybersecurity Technologies

Some public power utilities do not have the in-house capability to monitor for and alert on malicious activity on their network. These utilities often seek a Managed Security Service Provider (MSSP) to provide constant monitoring and to advise the utility on response and recovery from an incident.

APPA deployed IT monitoring devices and services at 43 public power utilities.

Task 3.1: Evaluate and deploy existing technologies and subscription services for public power utilities

Due to limited resources and personnel, it is often challenging for public power utilities to make informed security technology purchasing decisions. APPA engaged a consultant to evaluate existing technology and subscription services to allow utilities to compare options that would best serve the public power sector from both a technology and resource standpoint. Based on these findings, a self-sustaining subscription program was developed to deploy appropriate monitoring devices, which included subscription services, across a broader segment of public power. APPA solicited member cost sharing throughout the Project by encouraging members to apply for funding under APPA's Demonstration of Energy & Efficiency Developments (DEED) research and development grant program. The intent of using the Cooperative Agreement funds for this task was to incentivize and enable participation.

Task 3.1, Year 1: APPA evaluated various security and subscription service providers against public power utility security needs.

Year 1 results for Task 3.1

- Established a users group to identify and evaluate managed security service and subscription providers.
- Evaluated 48 providers, leading to identification of six managed security service providers as most appropriate to serve the needs of public power utilities.
- Conducted workshops to determine which providers public power utilities would most often choose.
- Initially, 15 utilities committed to deploy the N-Sentinel solution where an 80-20% cost share existed.

Year 1 key findings for Task 3.1

- From the selection of identified providers, public power utilities selected a provider based upon name recognition, existing experiences of other utilities, and/or the Hometown Connection partnership with APPA.
- Utilities with minimal expertise in cybersecurity service providers may be overwhelmed when offered too many options.
- Public power utilities often do not have the capacity to conduct a full solution analysis.
- Small public power utilities (and the people that managed them) lack an understanding

of cybersecurity technologies.
- Both cultural and financial barriers exist that hamper the willingness and ability to deploy new technology.
- Management and IT staff at the utility are not the sole stakeholders in terms of cybersecurity solution deployment; local elected and appointed officials are key in the decision-making process and even with an 80% subsidy, the remaining $2,000 was still a very high hurdle for some to overcome.

Task 3.1, Year 2: APPA continued to solicit public power utilities to share costs for this task by encouraging members to apply for funding under APPA's DEED program.

Year 2 results for Task 3.1

- Public power utilities were provided subsidies to install and test various technologies and subscription services.

A report was developed on the initial results of the N-Dimension installations, which. included lessons learned and recommendations for a future users group engagement.

Year 2 key findings for Task 3.1

- The majority of public power utilities do not have full time equivalent cybersecurity and IT staff.
- Public power utilities procure IT and cybersecurity services from different sources -- in-house, outsourced, and a mix of the two.
- Public power utilities that have some in-house capabilities reap the most benefit of vendor supplied cybersecurity technologies.
- Public power utilities that outsource their IT services use different contractual models with their service providers.
- Most public power utilities chose N-Sentinel’s N-Dimension subscription service based on name recognition.
- The results of installing the N-Dimension subscription service were mixed, depending on whether the utility had in-house information technology services or outsourced IT services.
- All public power utilities which installed the N-Dimension service found the technology at least somewhat improved their cybersecurity awareness and capability; many utilities noted great improvement.
- Public power utilities using the N-Dimension service had widely varying skill levels to manage digital assets and respond to N-Dimension’s reports and alerts.
- Many utilities found the N-Dimension reports and alerts too technical; while others thought the content was useful but lamented that the reports could have provided more information about what actions to take.
- The level of customer support by the vendor had a direct correlation to the degree of improvement in cybersecurity awareness and capabilities.
- Public power utilities have unique relationships with the municipalities they serve, which lead to unique technology deployments and associated challenges.
- The co-location of the utility with other municipal services (either in the same building or using the same switch) influences what network traffic is monitored.
- Most public power utilities have experience with just one MSSP and therefore will continue to use that provider.

Task 3.1, Year 3: The Cybersecurity Technology Assistance Program (CTAP) provided grants to public power utilities to offset up to 80% of the first-year costs of a cybersecurity technology solution, such as a MSSP to provide monitoring capabilities and alerts.

Year 3 results under Task 3.1

- Deployment of IPKeys – N-Dimension sensors at 25 utilities.

Year 3 findings for Task 3.1

- Partnering with a cybersecurity technology vendor is more efficient than allowing utilities to request a technology or service.
- Partnering with joint action agencies is an effective means to broaden awareness and interest in the program.
- Identifying the right point(s) of contact at utilities is essential.
- Many utilities are uncertain about their technology needs and would benefit from detailed guidance about commercial cybersecurity technologies and services.
- The level of technical expertise within a utility varies widely.
- Utilities frequently have short timetables to make purchases and need quick responses for their grant applications to budget accordingly.
- Lowering the cost barrier allows IT departments to make a purchase without approval from utility leadership.
- **Key Lessons for Public Power Utilities**
    - Leadership buy-in is essential.
    - Technical skills must be available and assigned to support the new technology.
    - Coordinate with third-party IT contractors early.
    - Set a baseline with a cybersecurity assessment.
    - Fine-tuning takes time and effort.
- **Considerations for Deploying Technology**
    - Identify existing vendors/service providers and technologies/services currently deployed.
    - Identify personnel capabilities, training, and awareness.
    - Identify scope, budget, deployment schedule, utility and/or municipal leadership approvals, and risks.
    - Secure training for management, technical, and general staff.
    - Update policies and procedures.
    - Incorporate tools into routines.
- The final report details findings for this task, including member feedback from a survey.

Task 3.2: Evaluate cyber risk information sharing and pre-commercial technology solutions at public power utilities

APPA intended to establish a team of technical experts from within public power utilities who would evaluate and begin to integrate security technologies at public power utilities, focusing specifically on identified technologies, such as the Schweitzer Engineering Laboratories (SEL) technology package and other devices from the national labs.

Task 3.2, Year 1: APPA hired a subject matter expert consultant to advise on Task 3.2 along with Tasks 4.1 and 4.2. The consultant helped analyze emerging technologies and existing commercial offerings. A final report, Public Power Cybersecurity Information Sharing Report, was developed under Task 4.1.

No pre-commercial technology was deployed. Task 3.2 deployment funds were rolled into Task 3.1 in Year 2.

Integrate ICE Calculator
A key part of understanding cyber risk is being able to quantify the potential cost of a cyber incident or attack. Not just the lost revenue to the utility, but the economic effects on the local community served by the utility. APPA integrated the Lawrence Berkeley National Laboratory's Incident Cost Estimator (ICE) calculator, which can be used to estimate the cost of a Ukraine-type cyber attack, into eReliability Tracker, APPA's proprietary reliability tracking software.

The eReliability Tracker is in use at more than 500 utilities.

Task 3.3: Subscriptions to eReliability Tracker for small APPA utility members

For utilities with fewer than 2,000 customers, APPA used Cooperative Agreement funds to help defray up to 80% of the cost of a 3-year subscription to the eReliability tracking service. It was intended that this effort reach up to 65 utilities and was offered on a first-come, first-served basis. This will help the smallest public power utilities transition from paper reliability records and participate in the APPA/DOE/Lawrence Berkeley National Laboratory (LBNL) research regarding resiliency and econometric evaluations of resiliency improvements in Task 3.4.

Year 1 results from Task 3.3

- 28 of the 65 identified small public power utilities were enrolled in the eReliability Tracker service.
- It was determined that the original limitation of this task to have only small public power utilities with 2,000 or fewer customers was too constraining, and the limitation was removed by DOE at the request of APPA.
- To increase enrollment levels, joint action agencies were asked to leverage the local influence they have with their public power utilities.

Year 1 key findings from Task 3.3

- Although interest has been high among potential eReliability Tracker subscribers, the engagement process has been longer than expected and the committal rate has been slow to grow.
- Internal review and purchasing processes within smaller public power utilities are slow, as decisions must be approved through a chain of decision makers.
- The smallest utilities, which have physically observable systems, likely do not have a need for eReliability Tracker services.

Task 3.3, Year 2: APPA continued to encourage its public power utilities to subscribe to the eReliability Tracker.

Year 2 results for Task 3.3

- In total 53 utilities enrolled in the subsidized 3-year subscription.

Year 2 findings for Task 3.3

- Once enrolled, public power utilities that use the eReliability Tracker are pleased with the

platform.

Task 3.3 Conclusion

The program was successful in signing up 96 public power utilities for eReliability Tracker subscriptions. These utilities utilized this platform to access the Ukraine cyber-attack scenario cost interruption estimate in Task 3.4.

Task 3.4: eReliability Tracker and Interruption Cost Estimate Calculator integration

APPA staff, in coordination with DOE and LBNL staff, developed and implemented advanced reliability and resiliency reporting algorithms and research. This research included 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 research was used to create predictive resiliency metrics, including cost estimates associated with outages that can assess the potential impact of cyber related events.

Year 1 results for Task 3.4

- Data was developed from the research conducted and used in Task 1.11.
- An extension was approved by DOE to have the report on the developed algorithms and research be submitted in September 2017.

Year 1 key findings for Task 3.4

- No key findings reported in Year 1.

Task 3.4, Year 2: APPA completed integration efforts of APPA's eReliability Tracker and the Interruption Cost Estimate (ICE) Calculator.

Year 2 results for Task 3.4

- ICE Calculator/eReliability Tracker integration was completed.

Year 2 findings for Task 3.4

- There is a lack of research into putting cyber in the context of reliability and operations.
- There are also research holes in terms of analyzing the effect of cyber-attack related corruption for the near and long term operational decision-making process at utilities.
- Manipulating utility data streams to cause attacker favorable effects in terms of operations is a threat that was explored on the reliability/resiliency side with the goal of publishing the results of the research in *Data Analytics for Energy, Water, and Environment IEEE Transactions on Engineering Management.*

Task 3.4 Conclusion

Since 11/27/2017 the program was successful in generating over 2000 ICE calculator reports for public power utilities that are new and existing eReliability Tracker subscribers.

Read more in the eReliability Tracker Interruption Cost Report.

Track Cyber Assets
An early indicator from the baseline assessments showed that public power utilities needed a way to track and assess their cyber assets. APPA developed a GIS-based Cyber Asset Tracker software for cataloging cyber assets and comparing the asset list to current vulnerability lists. At the conclusion of the Project, the software is in an alpha testing phase.

Task 3.5: Develop a Public Power Cyber Asset Tracker and Asset Information Management Methodology

New effort in Year 2

In September 2018, APPA and CrossCompute entered into an agreement to develop a Cyber Asset Tracker to help utilities better understand their cyber assets and prioritize cyber and physical improvements. In particular, this platform is intended for use by small and medium public power utilities that might not have the resources for an in-house geographic information system (GIS) staff to develop system maps or a large operational technology (OT) engineering staff to track potential vulnerabilities in OT assets.

Task 3.5, Year 2:

Cyber Asset Identification Methodology

APPA contracted with Burns and McDonnell to develop an asset identification methodology to help form the basis for the Cyber Asset Tracker. The methodology is presented in the *Asset Identification Methodology* report.

Cyber Asset Tracker Platform

The initial interface prototype was demonstrated at APPA's Engineering & Operations Technical Conference in Colorado Springs, Colorado in March 2019, with several attendees expressing interest in testing the system. An asset data gathering methodology was developed by Burns & McDonnell to establish guidelines for gathering and storing data locally in an automated fashion.

In Q3 of 2019, work focused on refining software integration, finalizing the build of the database schema, redeploying the web application, and completing authentication via APPA's OAuth2 code.

In July 2019, a contract extension was signed to continue work with additional milestones to further develop the asset tracker under Phase 2, focusing on improvements to cyber asset variable tracking and user experience refinements. Work on these deliverables continued throughout the remainder of 2019.

A no-cost time extension was signed in December 2019 to extend the period of performance through June 30 with the same Phase 2 deliverables.

The first user test with a new user was held in March 2020 to collect feedback on the user experience and identify any bugs.

A user test was held with APPA staff in late May 2020 to evaluate progress, test functionality, and collect feedback on changes to the user experience based on the previous user test in March.

Due to funding constraints requiring the re-allocation of funds, the project was closed out in August 2020. A final user test was held in mid-August with a larger number of APPA staff, which included testing the account log-in process and confirming all required functionality. The final

asset tracker version is 0.7.0 and a user tutorial video was recorded by CrossCompute: https://www.youtube.com/watch?v=CUJ3u_I282o

Task 3.4 Conclusion

The presentation of the initial interface prototype at the Engineering & Operations conference in 2019 validated utility interest in an affordable platform to track their cyber assets and alert them to vulnerabilities. A functioning version of the tracker was set to be demonstrated at the 2020 Engineering & Operations conference in April but was canceled due to the ongoing coronavirus pandemic.

The software is available on GitHub.

The Cyber Asset Tracker is currently in the alpha phase with basic functionality available. The next steps would be to conduct testing with member utilities to further refine the features and user interface based on feedback and observed use. This software would then be offered to public power utilities.

APPA recommends continued development of the cyber asset tracker into a platform for public release in order to meet the need for small and medium utilities to track their OT asset networks and improve vulnerability management and mitigation.

A final report was published for Task 3.5: Final Report

Task 4.0 Information Sharing

The Recipient will enable and encourage its members to participate in programs to develop and evaluate technologies needed to better share cyber and physical security threat information with other entities as well as the government. The Recipient will leverage its members for a broad range evaluation and integration of cyber risk information sharing platforms. The Recipient will develop case studies to inform public power entities on devices, tactics, and techniques best suited for their unique business model to promote information sharing, the Recipient may utilize a platform to communicate efficiently and securely resiliency and security risks to and among public power utilities and appropriate stakeholders.

Security Data Sharing

The myriad of threat and intelligence feeds can easily overwhelm any utility and digesting all of this information can be particularly burdensome for public power utilities that have small staffs or limited resources. APPA engaged trained cyber analysts to evaluate and digest threat data into a weekly report of actionable information.

Task 4.1: Evaluate information sharing tools and technologies

APPA evaluated information sharing tools and technologies that would improve the culture of cyber and physical resiliency and security within the public power community. These information-sharing methodologies incorporate a variety of technologies ensure interconnectivity with public and private partners in public safety, security, and community resiliency. APPA also evaluated secure platforms that will assist public power utilities in sharing sensitive information.

Task 4.1, Year 1: APPA began to evaluate information sharing tools and technologies to improve the culture of cyber and physical resiliency and security within public power utilities. APPA explored a risk-based framework for determining priority levels for the dissemination of secure messages and notifications to public power utilities.

Year 1 results from Task 4.1

- APPA identified and hired a consultant with expertise in secure information sharing tools and technologies.
- Conducted evaluation of potential secure information sharing platforms that best serve public power utilities. The results of the exploration identified several recommendations to the Electricity Information Sharing and Analysis Center (E-ISAC) to improve service for public power utilities.
- Encouraged public power utilities to sign up for the E-ISAC as the preferred source of threat information of the electricity industry.
- APPA also surveyed its utility members to determine the level of awareness and use of secure information sharing technologies among public power utilities.
- A final report, Cybersecurity Information Sharing Report, was developed.

Year 1 findings from Task 4.1

- APPA determined that a secure data sharing platform would be of benefit to members,

especially sharing of real-time threats between utilities.

- The survey results confirmed that, 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.
- The survey found that it is important for the E-ISAC to categorize, assess, disclose, and disseminate secure threat information that is useful and understandable for public power utilities.
- Many public power utilities do not have the software and hardware systems available to detect potential cyber threats. The JAAs could serve as a centralized repository for their utilities' security logs through the deployment of Security Event and Information Management (SEIM) tools. The JAAs could also serve as the broker of threat information from the E-ISAC to member utilities, filtering the threat information to be more actionable for the public power utilities.
- Due to the limited technical human resources available to public power utilities, there is an opportunity to leverage MSSPs to host secure SEIM solutions. The MSSPs can perform the day-to-day security event monitoring, ingest automated threat information from sources such as the E-ISAC, and notify the JAAs when there is suspect security event information that is actionable by public power utilities. The JAAs can then provide a mechanism to share anonymized and aggregated events back to the E-ISAC.
- In order to provide a robust secure information sharing program for public power utilities and integrate into the new E-ISAC automated indicatory sharing program:
    - Encourage public power utilities with the capability to start gathering security event logs to install a SEIM type solution. At a minimum, security logs should be correlated across the utility enterprise.
    - When the utility wants to share threat events externally, the SEIM should have the capability to use a secure transport method to establish a secure channel for exchange of the threat information using STIX/TAXII. This method allows a utility to send only the threat information versus providing full security event log information to other parties.
    - The E-ISAC should continue to develop the capability within its portal to send/receive threat information using the STIX/TAXII protocol.
    - 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.

Read more in the Cybersecurity Information Sharing Report.

Task 4.1, Year 2: Due to commitment to hurricane relief efforts, APPA was unable to evaluate information sharing tools and technologies that will improve the culture of cyber and physical resiliency and security within public power utilities during Year 2. Therefore, there are no results or findings for Year 2.

Task 4.1, Year 3: APPA developed two new programs to provide secure information sharing in a format that best serves public power utilities. First, APPA developed the Secure Data Sharing Program, which digested threat intelligence from various sources. Second, APPA developed the Shared Cyber Analyst Program to help utilities analyze and incorporate threat intelligence and mitigation at the local level.

Secure Data Sharing Program

In March 2019, EnergySec and APPA entered into an agreement to establish a "Secure Data

Sharing Program" as part of the multi-year cooperative agreement with the U.S. Department of Energy.

EnergySec worked with APPA to establish a users group to pilot a secure data sharing program, connecting participants via the ArmorText secure messaging platform and sharing curated threat information via a weekly newsletter.

To ensure a robust flow of threat intelligence, EnergySec and APPA identified and established connections to relevant information feeds, and established or formalized relationships with information sharing organizations such as the E-ISAC, Multi-State Information Sharing and Analysis Center (MS-ISAC), United States Computer Emergency Readiness Team (US-CERT), the Department of Homeland Security's Homeland Security Information Network (HSIN), the Federal Bureau of Investigation's InfraGuard, and the commercial monitoring service N-Sentinel sensors by IPKeys.

Analyst Services, Weekly Digests, and other Products

EnergySec provided cybersecurity analyst services to review and distill cybersecurity threat feeds and then relay actionable and usable information to APPA member organizations. EnergySec analysts were available for regular phone calls with APPA staff and pilot group participants, as needed, to explain, review, or expand on information provided.

Starting May 2019, EnergySec produced the Weekly Situation Report (WSR), which became a regular feature of the project.

EnergySec also produced special reports as warranted. In June 2019, EnergySec prepared three in-depth Technical Alerts on specific issues. In August 2019, EnergySec released an infographic highlighting the development of ransomware techniques over the preceding 30 years, including historical attacks against municipalities. In July 2020, EnergySec released a special report on phishing based on reports to the E-ISAC and a separate in-depth report on the Ripple20 vulnerabilities.

Technology Evaluation

EnergySec evaluated which technologies could develop, enhance, or deliver the products developed under this program, including secure messaging platforms and threat intelligence management platforms. EnergySec included feedback from the user's group regarding the usefulness of such technologies.

Threat Intelligence Platform

EnergySec used its access to the Anomali platform, including creating Trusted Circles for the sharing of indicators between pilot participants and other ISACS (e.g., MS-ISAC) and ISAOs, as well as the import of STIX/TAXII feeds where allowed (such as from E-ISAC).

ArmorText

The project used ArmorText, a secure messaging platform that features end-to-end encryption and other security features that is used by many electric sector organizations. EnergySec's role included designing and developing information products targeted at APPA's smaller utility members. The goal was to provide a consolidated view of relevant cybersecurity information customized for the public power community and in a form usable by smaller entities.

ArmorText is a secure messaging platform that provides a high level of trust for communication of sensitive cybersecurity information. While the WSR was produced at TLP: Green, the use of ArmorText allowed for discussions at the TLP: Amber level.

During the project, EnergySec was able to federate with several electric sector entities, allowing text communications with individuals on topics from the WSR and other reports. Although

overall interaction was relatively light, there were a few significant discussions and exchange of non-public documents that might not have occurred in the absence of this secure platform.

ArmorText was also tested as a platform for voice and video communications in an attempt to foster greater live discussion at higher levels of sensitivity. This was marginally successful with small groups and did result in some increased discussion. However, the ArmorText platform showed scalability issues that have not yet been addressed. For example, at times not all participants could hear all other participants. This limited the size of groups and the reliability of calls. Although the platform struggled in this area, future releases are promised to more robustly handle larger group calls, so a revisit on this topic may be warranted.

Weekly Situation Report

EnergySec produced the Weekly Situation Report from May 2019 through September 2020. In total, EnergySec delivered 62 issues of the report, which included 128 discussions of specific vulnerabilities, 68 discussions of current threats or campaigns, and 92 discussions on topics of strategic awareness.

Each week, EnergySec provided a live, 30-minute preview of the WSR with a discussion on each topic and the opportunity for Q&A from participants. The final WSR was released later in the week via email and ArmorText to participating public power entities.

EnergySec relied on various information sources in developing the WSR each week. These included open-source news feeds and non-public information from government and private sector partners. EnergySec gathered open-source information from a wide variety of news sources. The team configured Google News alerts and monitored RSS feeds from these sources and major security blogs (such as those by Dragos, Palo Alto Networks, and Cisco). The team also closely monitored public government information released through US-CERT, ICS-CERT, CISA, NCCIC, ICSJWG, DOE, and other agencies.

EnergySec also has access to non-public sources of information. Through a preexisting relationship with DHS, EnergySec has access to information released via the CSCP program, as well as AIS. Through a relationship with the Washington State Fusion Center, EnergySec received threat intelligence from the City of Seattle and Seattle City Light. Via a relationship with Anomali, EnergySec is provided access to the ThreatStream Threat Intelligence Platform, including numerous proprietary intelligence sources.

A final report was published for this portion of Task 4.1: Secure Data Sharing Program

Shared Cyber Analyst Program

Some public power utilities identified a need for onsite cybersecurity and IT services. APPA piloted a Shared Cyber Analyst Program in collaboration with a joint action agency (JAA) to provide small entities with additional local support in digesting threat information, offering training, conducting mitigation activities, and providing other cybersecurity services. The JAA will continue to provide this program as a service to its membership.

The program provided a cyber analyst to members of a regional municipal energy agency free of charge to help these small municipalities increase their cybersecurity preparedness. The cities' most pressing needs were Ransomware Readiness Guidance, MIL 1 Guidance, and Basic Incident Response Guidance. In supporting these goals, the program provided resources to the cities such as policy templates, a ransomware readiness questionnaire (RRQ), an asset inventory template, and free access to a commercial security awareness training platform.

The cities reported being excited to participate in a program that gave them direct contact with a cyber analyst free of charge. The program had significant participation, with 23 of 24 cities

(95.8%) participating in at least one aspect of the program, and only one that opted out. Twenty-one cities (87.5%) participated in more than one activity related to the program. Ten cities (41.7%) made progress on their Public Power Cybersecurity Scorecard. The overall Public Power Cybersecurity Scorecard improvement was low due to some cities which needed to implement other improvements before beginning the scorecard. In addition, the coronavirus played a part in delaying both involvement and improvements.

It was beneficial to have the cyber analyst check in periodically to ensure that cybersecurity did not become overlooked. The check-ins encouraged the cities to continue to make progress and allowed the cyber analyst to keep providing resources. Money and time are tight across the cities, especially with the coronavirus, so cyber improvements were slower than expected. Tightening budgets are a driving force behind why the program is so valuable to cities. They have the benefit of a resource free of charge to guide them on their cybersecurity journey.

The municipal energy agency's Board of Directors voted to continue funding the program as long as 75% of the cities participate in the program. With this funding, the program will evolve as the cities' needs change and will continue to be available at no additional cost to member cities.

Lessons Learned

- Cities mentioned that they did not know where to start. Providing a few recommendations at a time gives them a good place to begin and allows them to make positive changes without becoming overwhelmed by a complete list of items to accomplish.
- Cities, especially smaller cities, needed to complete basic cyber improvements before making Public Power Cybersecurity Scorecard improvements.
- A cybersecurity training program for city council members could be beneficial to show the importance of prioritizing cybersecurity in their city.
- If the Public Power Cybersecurity Scorecard costs money, cities will not use it.

The program has proven valuable to the municipal energy agency members. In addition to led to many of the cities implementing various security improvements. There has been significant participation in the program, and many of the cities mentioned how thankful they were to have the SCA program available to them free of charge.

A final report was published for this section of Task 4.1: Shared Cyber Analyst Program

Task 4.2: Evaluate Information Filtering Methodology

Due to limited resources, many utilities are unable to process efficiently the deluge of threat alerts, including how to identify and respond to the data that is important to them. APPA hired a consultant to explore a risk-based framework for determining priority levels for the dissemination of secure messages and notifications for public power.

Task 4.2, Year 1: A risk-based framework was explored for determining priority levels for the dissemination of secure messages and notifications for public power.

Year 1 results from Task 4.2

- Recommendations were developed and submitted to the E-ISAC on how to categorize, assess, disclose, and disseminate secure threat information that is useful and understandable for public power.

Year 1 key findings from Task 4.2

- Only 51% of public power utilities surveyed received external threat data.
- ***Year 1 effort completed – no further action needed; continued information filtering/sharing activities will be conducted under Task 4.1 in Years 2 and 3***
- A final report was developed for Task 4.2; *Public Power Cybersecurity Information Sharing Report*

Task 4.3: Develop resources for APPA utility members to facilitate engagement with associated constituents and other key stakeholders

APPA developed a security information engagement plan for public power utility managers to inform their colleagues, city officials and other key stakeholders. The focus of this engagement plan was 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 onboarding. This engagement plan will make it easier for utility managers to communicate with organizational leadership and state and federal partners when there are credible threats and concerns.

Year 1 results from Task 4.3

- APPA hired a consultant to develop a Security Information Engagement Plan for public power utilities.
- APPA and its consultant conducted two focus group sessions concerning public power engagement needs.

Year 1 key findings under Task 4.3

1. *Cyber Risk Environment*

   Cybersecurity at public power utilities is often scattered across senior management, information technology, operations, security, human resources, and other functional areas. In some cases, primary responsibility might not even reside within the utility.

   Cyber risk and threat information from internal and external sources tends to arrive in a splintered and ad hoc manner.

   There is a broad disconnect between what utility managers believe elected local government board members and executives want to know and when they want to know it, and the actual expectations of those individuals.

   Cybersecurity is a growing concern, and public power utilities might not have the resources to address it.

2. *Developing a Cybersecurity Program*

   A single individual should own cybersecurity. A “Cybersecurity Program Lead” should manage the process for cyber intelligence information flow within the organization. This is a critical first step in establishing sound protocols and information exchange around cyber.

   Utilities should assess their cyber risk through self-evaluation of risks, vulnerabilities, resiliency, and capabilities related to cyber. Tools such as the Public Power Cybersecurity Scorecard facilitate these assessments.

   All public power utilities should participate in cybersecurity training and scenario exercises. This should apply to anyone with access to the utility’s systems and should include both

onboarding and periodic refresher training.

Public power utilities should maximize their awareness of cyberthreats and actively monitor their networks.

All public power utilities should enroll in the Electricity Information Sharing and Analysis Center (E-ISAC).

Public power utilities should have a documented plan for escalating notification and reporting on cyber incidents. This should be equally robust as plans for escalating operational incidents.

Public power utilities should provide pre-incident outreach and education to local government leaders related to cyber. Such education should have two components: how an electric utility works and how cyberattacks can disrupt normal operations.

Local government leaders must be provided with reporting on cyberthreats and incidents without allowing sensitive information to be inappropriately exposed.

3. *Considerations for APPA and Industry Partners*
   - Deliver low-cost cybersecurity training and exercises.
   - Develop a road map to guide public power utilities in developing their cybersecurity programs.
   - Investigate how to develop the future security workforce.
   - Develop a public power cyber-response playbook.
   - Evaluate and deploy information-sharing tools and technologies.

- The final report was published: Security Information Engagement Plan for Public Power Utilities.
- ***Year 1 effort completed – no further action needed.***

Task 4.4: Improve Information Assurance in Communications

APPA assessed information assurance methodologies for data-in-motion and promoted adoption through training.

Task 4.4, Year 1: APPA hired a consultant to interview public power utilities and develop Information Assurance in Communications guidance document.

Year 1 results from Task 4.4

- Drafted and finalized assessment reports on the recommended methodologies, best practices and technologies to improve information assurance of data-in-motion.
- Drafted and finalized slide deck and presenter notes for promoting the adoption of the assessment recommendations by public power utilities.
- Conducted webinars to promote the adoption of the assessment recommendations.
- Drafted and finalized report describing three case studies of information assurance implementations at a small, medium and large public power utilities.

Task 4.4, Year 2:

Year 2 results for Task 4.4

- The report on information assurance in communications was completed.

- The report was delivered to 1,400 public power utilities.

Year 2 findings for Task 4.4

APPA published its report on Cybersecurity Information Assurance – Data Security Best Practices.

Cybersecurity Summit
Public power utility security personnel wanted a forum to network with peers and share lessons learned. APPA planned and delivered three national and three regional Cybersecurity Summits that offered this forum with a specific public power focus on cybersecurity practices and trends. More than 440 public power leaders and staff attended these summits.

Task 4.5: Plan a Public Power Security Summit

New effort in Year 2

APPA planned and delivered the first APPA Cybersecurity Summit on November 13-14, 2018. The purpose of the Summit is to provide public power utilities with the lessons learned from activities under the Project, provide networking opportunities among similarly situated public power utilities, and offer cyber and physical security educational opportunities.

Task 4.5, Year 2: APPA has planned the first National Cyber Summit to take place in November 2018. The purpose of the National Cyber Summit is to provide public power utilities with the lessons learned from activities under the Program, provide networking opportunities among similarly situated public power utilities, and offer cyber and physical security training opportunities.

Year 2 results of Task 4.5

- The first Public Power Cybersecurity Summit was held November 13-14, 2018 and had 159 attendees.

Task 4.5, Year 3: APPA continued the cybersecurity summits in Year 3 and expanded to produce three regional summits to address more local/regional issues. The regional summits remained focused on the foundational Program themes. APPA developed and delivered the second Public Power Cybersecurity Summit.

Year 3 results of Task 4.5

- Second Public Power Cybersecurity Summit was held November 19-20, 2019 and had 210 attendees.
- Three regional summits were delivered
    - Orlando, FL – Southeast Regional Summit, 99 attendees
    - Kearney, NE – Midwest Regional Summit, 72 attendees
    - Anaheim, CA – Western Regional Summit, 74 attendees

Task 4.5, Year 4: APPA continued to host a cybersecurity summit for public power professionals and other industry stakeholders. Due to the pandemic, in-person events were canceled or transitioned to a virtual format.

Year 4 results of Task 4.5

- Held third Public Power Cybersecurity Summit in a virtual format on November 16-18, 2020 with 229 attendees.

Task 5.0 Project Management and Reporting

The Recipient will develop and maintain a Project Management Plan (PMP) to foster team interaction, track deliverables, maintain a project timeline and milestone log, interface with DOE, and report progress and financials in accordance with the requirements set forth in the award document. Any proposed revisions to deliverables, milestones, the project schedule, or budget will be reported to DOE in accordance with the terms and conditions of the award. The PMP will be updated at least annually as part of the Continuation Application. The Recipient will prepare and submit quarterly project reports on program activities to DOE on a quarterly basis.

Task 5.1: Project Management Plan

APPA developed and revised its Project Management Plan (PMP) to track program activities, costing allocations, variances and projections, schedules, and other relevant information. APPA's Principal Investigator (PI) was responsible for the successful completion of the tasks within the PMP.

Task 5.2: Quarterly Reports

APPA produced quarterly progress reports and submitted to DOE.

Task 5.3: Continuation Application

An annual application was produced and submitted to DOE to continue the Cooperative Agreement.

Task 5.4: Annual Report

APPA produced an Annual Report and submitted to DOE.

Task 5.5: Data Management Plan

APPA submitted a Data Management Plan to DOE, per the requirements of the Cooperative Agreement.

Task 5.6: Prepare Materials for DOE Briefings

APPA developed presentation materials for DOE at kickoff meeting, quarterly meetings, and end of year meetings to indicate progress, budget status, and other agenda items.

STATEMENT OF PROJECT OBJECTIVES (SOPO)

American Public Power Association

Improving the Cyber and Physical Security Posture of the Electric Sector

A. Objectives

The Recipient will utilize its expertise in public power service, as well as its unique position as a community-owned electric utility convener to continue to promote a culture of security and resiliency within the public power community, and to coordinate with existing and future state/local/tribal/territorial and Federal programs. The Recipient will develop tools, educational resources, updated guidelines, and training on common strategies for fostering an improved resiliency and security culture at public power utilities. The Recipient will develop educational materials, case studies, secure communication platforms(s), and technical resources in coordination with the Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE) for dissemination to its membership with the purpose of enhancing organizational capacities. The primary objective of this initiative is to develop an internal cyber resiliency and security program at public power utilities.

B. Scope of Project

The Recipient will provide outreach, training, educational materials, exercises, workshops, site assessments, and technical assistance via in-person or virtual platforms to its membership of community-owned electric utilities to research and evaluate emerging technologies and support the development of cybersecurity guidelines that provide a baseline to protect against known vulnerabilities. The project supports efforts to: 1) advance development of cyber security tools and guidelines; 2) evaluate and mitigate cyber and physical system vulnerabilities; 3) research, develop, and adopt emerging technologies to improve resilience and security; and 4) enhance capabilities to share key information among public power providers. The tasks and activities to be performed will support the modernization of the Nation’s energy infrastructure, advancement and use of new energy technologies, and resilience of the nation’s energy system. The Recipient is encouraged to coordinate with other electric sector organizations, as appropriate throughout the project, to leverage resources and accomplish project objectives in an efficient and cost-effective manner.

C. Tasks and Subtasks to be performed

Task 1.0 Advancing Cyber Resiliency and Security Assessments

The Recipient will utilize the National Institute of Standards and Technology (NIST) Cyber Security Framework, DOE Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) tool, or equivalent as a baseline, to work with its membership to conduct assessments and develop a database to support ongoing benchmarking. The assessments will result in the development of a framework, guidelines, educational material, and the advancement of resiliency and security tools for public power providers.

Task 2.0 Onsite Vulnerability Assessments
The Recipient will conduct assessments and develop case studies of a segment of member entities. The Recipient will evaluate and integrate the processes and technologies available to alert public power utilities of threats and vulnerabilities in their cyber and physical systems and share results to drive continuous improvement.

Task 3.0 Extend and Integrate Technologies
The Recipient will engage with members to support adoption of promising technologies, develop case studies based on the emerging technologies, and share the information with appropriate stakeholders to meet emerging needs and create a more resilient energy delivery system. This includes extending, integrating, designing, and developing tools, technologies, and techniques that have the key properties of resiliency, real-time availability, integrity, authentication and confidentiality.

Task 4.0 Information Sharing
The Recipient will enable and encourage its members to participate in programs to develop and evaluate technologies needed to better share cyber threat information with other entities as well as the government. The Recipient will leverage its members for a broad range evaluation and integration of cyber risk information sharing platforms. The Recipient will develop case studies to inform public power entities on devices, tactics, and techniques best suited for their unique business model. To promote information sharing, the Recipient may utilize a platform to communicate efficiently and securely resiliency and security risks to and among public power utilities and appropriate stakeholders.

Task 5.0 Project Management and Reporting
The Recipient will develop and maintain a Project Management Plan (PMP) to foster team interaction, track deliverables, maintain a project timeline and milestone log, interface with DOE, and report progress and financials in accordance with the requirements set forth in the award document. Any proposed revisions to deliverables, milestones, the project schedule, or budget will be reported to DOE in accordance with the terms and conditions of the award. The PMP will be updated at least annually as part of the Continuation Application. The Recipient will prepare and submit quarterly project reports on program activities to DOE on a quarterly basis.

D. Technical Deliverables

All periodic and final reports will be submitted in accordance with the attached "Federal Assistance Reporting Checklist" and the instructions accompanying the checklist. In addition to the reports specified in the Federal Assistance Reporting Checklist, the Recipient shall provide the following to the DOE Project Manager identified in Block 15 of the Assistance Agreement cover page 30 days after an event or task is completed:

- Deliverable 1.0: The anonymized results of cyber security assessments, and the guidelines, educational material, and resiliency and security tools for public power utilities developed as part of the assessments.

- Deliverable 2.0: The anonymized results of onsite vulnerability assessments and associated case studies, reports, whitepapers, and/or briefs regarding processes and technologies available to alert public power utilities of threats and vulnerabilities in their cyber and physical systems developed as part of the vulnerability assessments.

- Deliverable 3.0: Case studies, products, papers, and reports developed in relation to the research, design, integration, installation, and development of emerging technologies.

- Deliverable 4.0: Products, papers, case studies, platforms and reports developed to inform public power entities on devices, tactics, resiliency and security risks, and techniques best suited for their unique business model.

- Deliverable 5.0: Project Management Plan, is due no later than forty-five days after award and submitted annually as part of the continuation application. In addition, updates or verification of the current PMP will be provided to the DOE Project Manager as required or needed. The PMP must be submitted in accordance with the format prescribed in SOPO Appendix 1 below.

- Deliverable 5.1: Documentation, prepared in accordance with the provision “Subaward/Subcontract Change Notification,” shall be submitted for each sub-award initially identified in the Recipient’s application as “to-be-determined.”

E. BRIEFINGS/TECHNICAL PRESENTATIONS

The Recipient will prepare detailed briefings for presentation to the Project Officer and Program Management at the Project Officer's facility located in Morgantown, WV or DOE HQ in Washington, D.C. (or at an alternate location approved by the Project Manager). Briefings will be given by the Recipient to explain the plans, progress, and results of the technical effort.

The Recipient must also provide and present project overview(s) and/or technical paper(s) at the Program Peer Review Meetings or other designated program meetings that are held annually, typically at the NETL facility located in Morgantown, WV or DOE HQ in Washington, D.C.