Improving the Cyber Resiliency and Security Posture of Public Power

1. EXECUTIVE SUMMARY AND TECHNICAL APPROACH

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

Mid to small sized public power utilities may have unique organizational structures with regard to operations, systems control and monitoring, internal or city information technology departments, leadership/governance, and use of third party service providers. These structures may not lend themselves to immediate recognition of threats and the escalation of potential incidents. These nuances may also require additional education, coordination, capability building, and pre-established resources to set proper expectations among all stakeholders, to monitor and detect threats, to maintain situational awareness among decision makers, and to respond properly to threats and indicators of varying degrees.

FUNDING

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

OBJECTIVES

The objective of this multi-year, multi-task project is to improve the cyber resiliency and security posture of public power. APPA will provide its members with a multitude of security tools, technologies, and programs so that the public power community is better able to understand, install, and implement new cyber and physical resiliency and security systems. Under the project, APPA will coordinate with existing and future state/local/tribal/territorial and Federal programs. APPA will oversee all aspects of the project; however, due to its limited staff resources as a member supported organization, it will supervise consultants to undertake most of the tasks outlined in the Project Management Plan (PMP).

SCOPE OF PROJECT

APPA will undertake, at a minimum, four multi-pronged tasks to include 1) Efforts to advance cyber resiliency and security assessments; 2) Conduct, evaluate, and use the results of on-site vulnerability assessments; 3) Research, evaluate, deploy, and integrate both commercial and pre-commercial security technologies; and 4) Research, evaluate, and implement information sharing mechanisms. APPA will also explore the feasibility of secure communication mechanism adoption(s).

The purpose of completing these tasks is to deploy technologies, develop tools, write and disseminate

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

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

educational resources, update guides, conduct training sessions, and undertake outreach efforts. The objective of these strategies is to foster a cyber and physical resiliency and security culture at public power utilities. The educational materials may include reports, key findings from assessment results, case studies, meeting summaries, webinars, recommendations and frameworks to increase the resiliency and security capabilities of its member utilities.

The PMP outlines the tasks that will begin, but necessarily be completed in Year 1 of the project. Under the direction of DOE, tasks may be revised and/or added in years 2 and 3, if funds and resources permit. Additionally, APPA will coordinate with the National Rural Electric Cooperative Association (NRECA), the North American Electric Reliability Corporation (NERC) and other organizations, as appropriate, to complete the tasks.

PROJECT OUTLINE

Task 1.0 Advancing Cyber Resiliency and Security Assessments

1.1: Conduct baseline assessments

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

1.3: Develop Public Power Resilience and Security Maturity Model

1.4: Develop targeted security training opportunities

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

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

1.7: Explore procurement mechanisms

Task 2.0 Onsite Vulnerability Assessments

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

Task 3.0 Extend and Integrate Technologies

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

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

3.3: Subscriptions to eReliability Tracker for small APPA utility members

3.4: eReliability Tracker and Interruption Cost Estimate (ICE) Calculator integration

Task 4.0 Information Sharing

4.1: Evaluate information sharing tools and technologies

4.2: Evaluate threat information filtering methodology

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

4.4: Improve Information Assurance in Communications

Task 5.0 Project Management and Reporting

5.1: APPA will hire an outside consultant for project management activities

PROJECT MANAGEMENT PLAN (PMP)

2. KEY PERSONNEL

- Michael Hyland, Senior Vice President, Engineering Services
- Nathan Mitchell, Senior Director, Electric Reliability Standards & Security
- Alex Hofmann, Director, Energy and Environmental Services
- Tanzina Islam, Energy and Environmental Services Manager
- TBD, Engineering Services Security Specialist
- Patricia Keane, Engineering Services Specialist
- Kegan Gerard, Engineering & Operations Assistant

4. PROJECT OUTLINE

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 1.1: Conduct baseline assessments

Using the NIST Cyber Security Framework, DOE ES-C2M2 tool or equivalent, APPA will seek input from a statistically significant sample of public power utilities to baseline existing cyber and physical resiliency and security capabilities and better define the current resiliency landscape in public power. The results of this baseline survey will inform future activities related to this effort, and will be critical for the development of a public power security framework. To obtain this information from public power utilities, APPA will utilize a consultant to conduct facilitated meetings, surveys, phone calls, and/or other means of outreach.

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

APPA will utilize a consultant with expertise in analyzing demographic data to compile the results of the baseline assessments in Task 1.1. The contractor will identify ways to categorize public power utilities based on security and resilience capabilities, risk, and/or size. These categories will inform the development of the Public Power Resilience and Security Maturity Model, accounting for the unique posture and capabilities of public power utilities. Under the overarching resiliency title, both cyber and physical vulnerabilities need to be addressed.

Task 1.3: Develop Public Power Resilience and Security Maturity Model

Following the baseline resiliency assessments and subsequent demographic analysis, APPA will develop the Public Power Resilience and Security Maturity Model for public power communities. The Model will factor in relevant NERC standards, NIST Cyber Security Framework, and DOE ES-C2M2 to develop a maturity model framework relevant to public power. The Model will enable public power utilities to understand the characteristics of mature cyber and physical resiliency and security programs, processes, and tools, and help them enhance their programs based on their organizational structure and risk profile. APPA will investigate collaborating with NRECA on this task if it is found to be mutually beneficial and cost effective.

Task 1.4: Develop targeted training opportunities

APPA will conduct training sessions related to the unique cyber and physical resiliency and security posture of public power. Several of these training sessions will be conducted in tandem with public power conferences, as well as via webinars and online training modules. APPA may utilize professional trainers with expertise in areas identified as needing further training on cyber and physical cyber resiliency and security. At the conclusion of these efforts, APPA will work with a consultant to develop a report to evaluate the courses, instructors, and determine the most efficient direction for future training offerings.

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

APPA will facilitate technical workshops, exercises and/or roundtable discussions to challenge assumptions and test out models developed in this Project. These exercises are intended to reach a wide variety of audiences and perspectives to gather additional insight into the characteristics and processes unique to public power utilities. APPA will engage the services of a consultant who will develop and facilitate all aspects of these sessions, which will be conducted throughout the Project period of performance.

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

APPA will develop short, actionable videos and/or presentation materials to educate first responders, city officials, and other stakeholders in public power communities on security issues related to the electrical system. A subject matter expert will be engaged to oversee this task, select a production company, and work with APPA on content and audience selection. These materials should be made available in a manner that allows individual utilities and groups to customize them to suit their unique needs (when feasible).

Task 1.7: Explore procurement mechanisms

APPA will conduct an initial analysis of current cyber and physical security and resiliency technologies and match those technologies to classes of public power utilities with the capability to implement these technologies. Based on the results of the initial analysis, APPA may develop procurement mechanisms that can be used by public power utilities. A user guide will be included with the deliverable. APPA will investigate collaborating with NRECA on this task if it is found to be mutually beneficial and cost effective.

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

In Year 1 of the Project, APPA will begin to conduct initial cyber and physical resiliency and security assessments of public power utilities across a variety of demographics. The assessments may continue into Years 2 and 3 of the Project, but are dependent on future funding for broadest coverage. These assessments are intended to explore the varying conditions and operating realities present throughout different segments of the public power community, and how these unique characteristics affects the maturity and effectiveness of cyber resiliency and security programs. APPA will engage the services of a consultant to develop and conduct these assessments. The consultant will evaluate systems against existing resources including, but not limited to, APPA's Physical Security Essentials Guidebook, APPA's Cyber Security Essentials Guidebook, eReliability tracker program, and will share the findings in aggregate.

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.

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

APPA will engage a consultant to conduct an evaluation of existing technology and subscription services, including the N-Dimension N-Sentinel technology, for comparing 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 may be developed during the Project performance period to deploy appropriate monitoring devices, which will include subscription services, across a broader segment of public power. APPA will solicit 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 is to incentivize and enable participation. A user group will be formed to provide feedback on possible deployments. The user group will work with a consultant to develop a report evaluating the sustainability of the subscription program, recommendations for enhancements to the technology that would benefit the public power community, and ideas for future research needed to develop the technology. The activities under this task will be completed at the end of the Project performance period.

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

APPA will establish a team of technical experts from within its member utilities who will evaluate and begin to integrate resiliency, cyber and physical resiliency and 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. To accomplish this, APPA will hire a subject matter expert to manage the team's efforts that will be conducted over the Project performance period. The team will coordinate with members to evaluate existing deployments of technology solutions. The team will analyze emerging technologies and existing commercial offerings to develop a catalogue of solutions that may be useful for deployment at public power utilities. Using the demographic data, along with an understanding of the maturity levels of members, the team may recommend classes of technologies that are appropriate for the maturity level of a public power utility. During the project performance period, these technology solutions will be deployed at various public power utilities and evaluated by a users group.

3.3: Subscriptions to eReliability Tracker for small APPA utility members

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

3.4: eReliability Tracker and Interruption Cost Estimate (ICE) Calculator integration

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

Task 4.0 Information Sharing

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.

4.1: Evaluate information sharing tools and technologies

APPA will evaluate information sharing tools and technologies that will improve the culture of cyber and physical resiliency and security within the public power community. These information-sharing methodologies may incorporate a variety of technologies to reduce the time burden placed on the reporting entities, while ensuring interconnectivity with public and private partners in public safety, security, and community resiliency. APPA will engage an information sharing platform expert to help evaluate and make recommendations on secure platforms that will successfully assist public power.

4.2: Evaluate Information Filtering Methodology

Due to limited resources, many utilities are unable to efficiently process the deluge of threat alerts, including how to identify and respond to the data that is important to them. Once unique demographic groups are identified under Task 1, APPA will hire a consultant to explore a risk-based framework for determining priority levels for the dissemination of secure messages and notifications for public power. The consultant will develop recommendations for E-ISAC on how to categorize, assess, disclose, and disseminate secure threat information that is useful and understandable for public power. Secure information should include near real-time documentation of key threat indicators and actions taken to date by the reporting entity. The consultant will develop a report that addresses key findings of how public power will be able to use various levels of secure information.

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

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

APPA will hire a consultant to conduct the engagement that will be undertaken throughout the Project performance period.

4.4: Improve Information Assurance in Communications

APPA will assess information assurance methodologies for data-in-motion and promote adoption, as appropriate.

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.

5.1: Project Management Plan

APPA will develop this Project Management Plan (PMP) to track program activities, costing allocations, variances and projections, schedules, and other relevant information. APPA's Principal Investigator (PI) will be responsible for the successful completion of the tasks within the PMP. The PI will hire a consultant who will be responsible for all tracking and reporting requirements of project management.

5.2: Quarterly Reports

APPA will produce quarterly progress reports and submit to DOE.

5.3: Continuation Application

An application will be produced and submitted to DOE to continue the Cooperative Agreement.

5.4: Annual Report

An Annual Report will be produced by APPA and submitted to DOE.

5.5: Data Management Plan

APPA will submit a Data Management Plan to DOE, per the requirements of the Cooperative Agreement. The APPA Data Management Plan will outline the data that will be shared, preserved, digital research data, and research data. APPA will validate all data provided.

5.6: Prepare Materials for DOE Briefings

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

6. METRICS AND BENEFITS

Task #	Task	Metrics	Benefits	Reporting	
				Frequency	**Format**
1	**Advancing Cyber Resiliency and Security Assessments**	# of assessments completed and # of copies of report disseminated	Increased knowledge of status of resiliency and security capabilities among public power utilities	Quarterly	Progress Report
2	**Onsite Vulnerability Assessments**	# of assessments completed	Identification of best practices, needs, gaps and increased information exchange	Quarterly	Progress Report
3	**Extend and Integrate Technologies**	# of installations of commercial and pre-commercial technologies	Increased cyber resiliency and security within the public power community	Quarterly	Progress Report
4	**Information Sharing**	# of users of new information sharing methodologies; # of users of new information filtering technology; # of copies of educational materials distributed	Public power community will have increased ability to share and filter information securely; educational materials will inform associated constituents	Quarterly	Progress Report
5	**Project Management and Reportin**g	# of Progress Reports and Annual Report	Lessons learned from project will serve as basis for future R&D	Quarterly	Progress Report

7. RISK MANAGEMENT

Risk Management Log		
Risk	**Impact**	**Mitigation Method**
APPA personnel changes may take place during project period of performance	LOW: Knowledge base could be disrupted	APPA will ensure that a team approach is used so that there are back-up personnel in place, and will supplement with new personnel as needed
Commercial and pre-commercial technologies selected for pilot programs may not produce strong results	LOW: Pilots are meant to result in lessons learned	If pilot program is not going well, APPA and its contractors will revise or stop program early
Lack of widespread use of new tools and protocols	LOW: It will take time for public power utilities to have a comfort level with new tools and protocols	APPA will strive to ensure that public power utilities adopt new tools and technologies through training seminars, webinars, case studies, and other outreach activities
Underperforming consultants	LOW: Delay in deliverables and/or milestones	Clear and rigorous RFPs and strong contractual provisions will be drafted to select candidates that can adequately provide needed services; strenuous oversight will be taken by APPA management
Incomplete funding of entire project	HIGH: Without funding all three years of project, the project will be unable to produce intended R&D	APPA will work closely with DOE during Year 1 to ensure project requirements are met and to provide basis and reasoning for future funding
Major cyber or physical security event happens	HIGH: All APPA staff will be expected to focus all efforts in support of member response to event	APPA will strive to ensure that all technical consultants are capable of completing tasks on their own in case of a major event

8. STATEMENT OF PROJECT OBJECTIVES (SOPO)

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.

- 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.