


Improving the Cyber and Physical Security Posture of Public Power



Enhancing a culture of security and resiliency at community-owned electric utilities

Keeping America's critical infrastructure secure from increasing threats—whether cyber or physical attacks—is a shared priority of American Public Power Association (APPA) members involving 2,000 local- and state-owned electric utilities across the U.S. To assist these utilities, which serve approximately 15% of electricity customers, the APPA developed a program to advance the culture of cybersecurity and resiliency. This project provides the public power community with a multitude of tools, technologies, and training to understand, install, and implement resilient cyber and physical security systems. The program includes outreach, training, exercises, workshops, technology deployment, assessments, and technical assistance for public power utilities. The project develops right-sized cybersecurity tools and guidelines; evaluates and mitigates cyber and physical system vulnerabilities; researches, develops, and adopts emerging technologies to improve resilience and security; and enhances capabilities to share information among public power providers.

KEY TAKEAWAYS

- Increases public power utilities' awareness of their cybersecurity risk via assessments and accessible resources
 - Facilitates utilities' risk mitigation and cybersecurity maturity planning
 - Enables practicable cyber threat information sharing appropriate to utility size and scope for ongoing vigilance
- 

OUTCOME

Small to medium public power utilities each have unique organizational, leadership, and governance structures to manage operations, system controls, monitoring, and information technology – each which might include city managed IT/OT networks and third-party service providers. These structures may not lend themselves to the recognition of cyber threats and immediate escalation of potential incidents. This project enabled APPA to develop assessments to help move the needle on the maturity level of small to medium utilities, deploy resources to protect critical infrastructure, develop a curated set of resources to help utilities set a path of continuous improvement and information sharing.

PARTICIPANTS

ROLE



Overall program leadership and coordination with public power utilities to develop tailored cybersecurity resources that fit their unique needs.



Develops the cybersecurity scorecard online portal for public power utilities to self-assess their cybersecurity program based on the foundational practices of the DOE Cybersecurity Capability Maturity Model.



Develops a cybersecurity roadmap to guide public power utilities in improving their cybersecurity program maturity.



Develops a cyber incident response playbook to give public power utilities guidance on how to respond and recover from a cybersecurity event.



Onsite assessments to get a deep dive into public power utility cybersecurity program and controls.



Deploys cybersecurity monitoring systems to give public power utilities insight into cyber incidents and alert them to malicious activity on their IT networks. The Cyber Technology Assistance Program provides 80% cost coverage on new deployments.



Develops a process to analyze and securely exchange threat intelligence and encourage sharing between public power utilities.



Develops a cyber analyst who can support a group of small public power utilities in a state or region.

CONTACT INFORMATION

Nathan Mitchell
Principal Investigator
American Public Power Association
202-457-2925
NMitchell@PublicPower.org

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: July 2016 – September 2020

Total Award Value: \$7,906,121
DOE Share: \$7,500,000
Cost Share: \$406,121

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: <https://www.energy.gov/ceser>

Date Written: June 2021