AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

ISSUE BRIEF January 2023

Grid Security

- The electric sector has mandatory and enforceable federal regulatory standards in place for cyber and physical security (collectively known as grid security).
- Close coordination among industry and government partners at all levels is imperative to deterring attacks and preparing for emergency situations.
- The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) should be implemented in a risk-based manner and harmonized with existing reporting requirements.

Background – The Key Pillars of Grid Security

Mandatory and Enforceable Standards

Congress approved the mandatory and enforceable standards regulatory regime for the bulk power system in the Energy Policy Act of 2005 (EPAct05) (section 215 of the Federal Power Act (FPA)). Under section 215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities, and government representatives, regularly drafts reliability, physical security, and cybersecurity standards that apply across the North American grid, including Canada. Participation by industry experts and compliance personnel in the NERC critical infrastructure protection (CIP) standards development process ensures that the standards are technically sound, fair, and balanced. The Federal Energy Regulatory Commission (FERC) has the power to then approve or remand those standards as they apply in the United States. To ensure compliance, under FERC's oversight, NERC and its regional entities conduct rigorous audits and can levy substantial fines for non-compliance. Additionally, FERC can instruct NERC to develop new or revised reliability standards with a very short turn-around time. CIP standards establish an important baseline of security—but they are a floor, not a ceiling—and grid security is and should be much more than a compliance exercise.

Information Sharing and Protection

The electric sector is unique in that it has long been subject to cyber incident reporting mandates to the Department of Energy (DOE) via an Electricity Emergency Incident and Disturbance Report (OE-417) and NERC/FERC. Moreover, there is robust electric utility industry participation in information sharing organizations known as the Electricity Information Sharing and Analysis Center (E-ISAC) and the Multi-State Information Sharing and Analysis Center.

Another layer of mandatory cyber incident sharing requirements will be added through CIRCIA. Signed into law in March 2022, CIRCIA will require covered critical infrastructure entities to report cyber incidents within 72 hours and ransomware payments within 24 hours to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The law gives CISA significant discretion in implementation, including defining what constitutes a covered entity. APPA filed comments in response to a request for information kicking off the CIRCIA rulemaking asking CISA to take a careful and deliberative approach to implementation, taking into account existing reporting mandates and organizations, and to appropriately tailor reporting mandates commensurate with risk to national security.

The ability to protect sensitive electric information from public disclosure is critical to grid security. The Fixing America's Surface Transportation Act of 2015 or "FAST Act" (Sec. 61003 of P.L. 114-94) gave the Secretary of Energy broader authority to address grid security emergencies under the FPA and clarified the ability of FERC and other federal agencies to protect sensitive critical electric

infrastructure information (CEII) from public disclosure under the Freedom of Information Act and other sunshine laws. Under the FAST Act, FERC-designated CEII is exempted from disclosure for a period of up to five years with a process to lift the designation or challenge it in court. In addition, it established sanctions for the unauthorized disclosure of shared information. It is critical to operational security that the industry is confident that sensitive information about critical infrastructure that might provoke new threats or endanger the integrity of the electric power grid not be publicized. CEII in the public sphere creates a grave vulnerability to the electric power grid by significantly reducing the surveillance effort required by dedicated domestic and foreign adversaries. APPA has supported legislation and actions by DOE and FERC that would further clarify and enhance the responsibility of the federal government and other stakeholders to maintain the confidentiality of CEII to minimize the risk that such information could be used by malicious actors to target grid infrastructure.

Public-Private Partnerships

The electric power industry works closely with the federal government, including NERC, FERC, DOE, and DHS, on matters of critical infrastructure protection. One important venue for this collaboration is the Electric Subsector Coordinating Council (ESCC). The ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. APPA and public power utilities play a leadership role on the ESCC, which includes utility CEOs and trade association leaders representing all segments of the industry. Their counterparts include senior administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

APPA works closely with DOE on a number of fronts. Notably, APPA has been awarded three grants since 2016 to help strengthen the cybersecurity posture of public power utilities. Most recently, in September 2022, DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) awarded APPA a grant of $15 million over a three-year period to facilitate the adoption and deployment of industrial control systems cybersecurity technologies for municipal utilities. This builds off an existing $6 million, three-year cooperative agreement (awarded in 2020) to develop and deploy cyber and cyber-physical solutions for public power utilities, and a previous three-year cooperative agreement (awarded in 2016) to assist small- and medium-sized public power utilities with cyber risk assessment and cybersecurity training.

A new program at DOE, the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC), which passed as part of the Infrastructure Investment and Jobs Act (P.L. 117-58), is based off the successes of these grant programs. The RMUC is authorized to appropriate a total of $250 million in grants and technical assistance over five years to rural, municipal, and small investor-owned electric utilities to enhance their security posture. APPA and many public power utilities are expected to benefit from this program.

"Defense-in-Depth" and Sector-Wide Preparation Exercises

The goal of every utility and the entire industry is to manage risk prudently. Still, there are tens of thousands of diverse facilities throughout the U.S. and Canada that cannot be protected 100 percent of the time from all threats, requiring utilities to prioritize facilities and assets that, if damaged, would have the most severe impacts on their ability to keep the power on. As such, the electric power industry employs threat mitigation known as "defense-in-depth" that focuses on preparation, prevention, response, and recovery to "all hazard" threats to electric grid operations.

Electric utilities plan and regularly exercise for a variety of emergency situations that could impact their ability to provide electricity. One of the biggest exercises, GridEx, takes place every two years. GridEx VI took place in November 2021 and involved hundreds of organizations and thousands of participants from industry, government agencies, and partners in Canada and Mexico. Managed by NERC and the E-ISAC, the event included a tabletop exercise where electric sector executives and senior government officials worked through incident response protocols in a scenario involving multiple operating challenges.

The three primary segments of the electric utility industry—public power, investor-owned, and rural electric cooperatives—have long had in place mutual aid response networks to share employees and resources to restore power after natural disasters and other emergencies. The ESCC used the concept of traditional mutual assistance networks to develop the Cyber Mutual Assistance program that can help electric and natural gas companies, public power utilities, and/or rural electric cooperatives restore critical computer systems following significant cyber incidents. The program now includes 175 entities across all segments of the industry, serving more than 80 percent of all U.S. electric customers.

Finally, electric utilities regularly share transformers and other equipment through long existing bilateral and multilateral sharing arrangements and agreements. The industry is expanding equipment sharing programs—like the Spare Transformer Equipment Program (STEP), SpareConnect, and Grid Assurance—to improve grid resiliency.

APPA Contacts

Amy Thomas, Senior Government Relations Director, 202-467-2934 / athomas@publicpower.org

Bridgette Bourge, Senior Director, Cybersecurity, 202-467-2925 / bbourge@publicpower.org