AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

ISSUE BRIEF June 2025

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.
- Congress should expeditiously reauthorize the Cybersecurity and Information Security Act of 2015 (CISA 2015) to ensure that the legal structure for the voluntary sharing of information between and among the federal government and private entities remains in place.
- Congress should postpone consideration of legislation to create additional cyber incident reporting mandates for the energy sector until the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) is fully implemented.

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 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). In March 2024, CISA released a notice of proposed rulemaking (NOPR) to begin implementing CIRCIA. APPA is concerned that the

NOPR is overbroad with respect to reporting requirements for small, distribution-only electric utilities. While reporting obligations are appropriate for large utilities that serve millions of customers, it is unnecessary and burdensome to impose the same obligation on hundreds of community-owned electric utilities that serve fewer than 2,000 customers each and pose a negligible risk to the reliability of the broader grid. APPA is also concerned that CISA is moving forward with its rule without having finalized plans and agreements to avoid duplicative reporting requirements. Prior to issuing a final rule, APPA believes that CISA should complete its consultations with DOE and FERC and enter an information sharing agreement with them.

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, 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 is not 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.

Finally, CISA 2015 set up policies and procedures for voluntary sharing of cybersecurity threat information between and among the federal government and private entities (the definition of which includes public power utilities) and provides limited liability protection for these activities.

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 Electricity 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 several fronts. Notably, APPA has been awarded four grants since 2016 to help strengthen the cybersecurity posture of public power utilities. APPA is currently executing a grant of $15 million over eight years from DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to facilitate the adoption and deployment of industrial control systems cybersecurity technologies for municipal utilities. This builds off an existing $6 million, seven-and-a-half-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.

The Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC) Program, 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 Program 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. In 2024, APPA was awarded a $4 million grant to launch the Cyber Pathways program to improve the cybersecurity posture of public power utilities with limited resources, serving military installations, or are critical to the bulk-power system. President Trump's fiscal year 2026 budget request proposes to rescind $166.1 million in unobligated RMUC funds. APPA believes that the program is a generational opportunity to improve the cybersecurity of under-resourced, not-for-profit utilities and that the proposal to rescind funds is unwarranted.

"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. Managed by NERC and the E-ISAC, GridEx VII will take place this November and will involve hundreds of organizations and thousands of participants from industry, government agencies, and partners in Canada and Mexico.

Building off the success of GridEx, APPA will host its first ever cyber mutual aid exercise, Safe Haven, in fall 2025, funded by DOE. Safe Haven will be held in Washington and Kansas, locations that were selected in coordination with DOE based on several criteria. The scenario will feature a cyber event that has physical impacts to the grid. APPA is working in close coordination with the E-ISAC to help drive participation by smaller utilities that do not usually participate in GridEx and to provide them with lessons learned to incorporate into the biennial exercise.

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 200 entities across all segments of the industry, serving more than 85 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, SpareConnect, and Grid Assurance—to improve grid resiliency.

Congressional Action

In May 2025, Senators James Lankford (R-OK) and Gary Peters (D-MI) introduced S. 1875, the Streamlining Federal Cybersecurity Regulations Act. The bill would establish an interagency Harmonization Committee at the Office of the National Cyber Director (ONCD), which is housed in the White House, and would require the committee to develop a framework for the alignment of cybersecurity and information security regulations, rules and compliance requirements. It would also require that all agencies, including independent regulatory agencies, consult with the committee before issuing or updating regulations. APPA strongly supports the goals of the bill.

As noted above, CISA 2015 set up policies and procedures for the voluntary sharing of cybersecurity threat information between and among the federal government and private entities and provided limited liability protection for these activities. The law will expire on September 30, and APPA is part of a coalition of critical infrastructure sectors advocating for the law's extension. Senators Mike Rounds (R-SD) and Gary Peters (D-MI) have introduced legislation (S. 1337) to extend CISA 2015 for ten years; APPA strongly supports S. 1337.

APPA Contacts

Amy Thomas, Vice President of Government Relations, 202-467-2934 / athomas@publicpower.org

Michael Coe, Vice President of Physical and Cyber Security Programs, 202-467-2956 / mcoe@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 and protect the interests of the more than 55 million people that public power utilities serve and the 100,000 people they employ.