AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

ISSUE BRIEF June 2021

Grid Security

Summary

A reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans. Public power utilities, together with the entire electric utility industry, take very seriously their responsibility to maintain a secure and reliable electric grid. It is the only critical infrastructure sector that has mandatory and enforceable federal regulatory standards in place for cyber and physical security (collectively known as grid security). Cyber-attacks, relatively new compared to long-known physical threats, have rapidly evolved and could have operational consequences. The American Public Power Association (APPA) believes that the industry and its federal government partners have made great strides in addressing cybersecurity threats, vulnerabilities, and potential emergencies. Given the persistence and sophistication of threats, APPA knows that utilities cannot prevent all attacks at all times. For both cyber and physical threats, electric utilities employ risk management programs to prioritize facilities and equipment, develop contingency plans, and employ defense-in-depth techniques to keep the lights on.

Key Pillars of Grid Security

Mandatory and Enforceable Standards

The electric utility sector is the only critical infrastructure sector (besides the nuclear power sector, a part of the overall sector) that has a mandatory and enforceable federal regulatory regime in place for cybersecurity. Congress approved the standards 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.[1] 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

Industry has long recognized that increased information sharing and appropriately tailored liability protection would further enhance the industry's ability to guard against cyber-attacks. As such, APPA strongly supported passage of the Cybersecurity Act of 2015, which was incorporated as Division N of

1 NERC standards cover the Bulk Electric System (BES).

P.L. 114-133, the Consolidated Appropriations Act, 2016. The act provides policies and procedures for sharing cybersecurity threat information between the federal government and private entities (which includes electric utilities), as well as sharing between private entities while providing limited liability protection for these activities if conducted in accordance with the act.

In addition to the Cybersecurity Act of 2015, APPA also strongly supported section 61003 of P.L. 114-94 (the Fixing America's Surface Transportation Act or "FAST Act"), which gave the Secretary of Energy broader authority to address grid security emergencies under the FPA. It also 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 (FOIA) 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 information 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 ability 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.

APPA strongly encourages its members to share physical security and cybersecurity related threats that they face to information sharing entities, such as the Electricity Information Sharing and Analysis Center (E-ISAC), as well as the Multi-State Information Sharing and Analysis Center. These information sharing organizations are critical to ensure that the broader public power community and the entire electric power industry have awareness of the tactics, techniques, and procedures used by the adversaries targeting the electric grid.

Public-Private Partnerships

The electric power industry works closely with the federal government, including NERC, FERC, DOE, and the Department of Homeland Security (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 directly with DOE on a number of fronts. Most recently, in September 2020, DOE's Office of Cybersecurity, Energy Security and Emergency Response (CESER) awarded APPA a grant of $6 million over a three-year period to develop and deploy cyber and cyber-physical solutions for public power utilities. The program's goal is to provide utilities with emerging innovations at the hardware, firmware, and/or software levels to protect key operation technology (OT) components that enable the safe control of the physical systems that deliver electric power. This effort builds on the accomplishments of another three-year grant CESER awarded to APPA in 2016, with which APPA assessed and helped to strengthen the cybersecurity posture of small- and medium-sized public power utilities. This grant enabled the development of a cybersecurity scorecard for public power utilities to assess their cyber readiness, the production of a cybersecurity roadmap, an incident response playbook, and other guidance documents to help utilities develop a culture of cybersecurity within their organization.

Legislation based on the success of the 2016 grant program has been introduced over the past three Congresses. Most recently Representatives Jerry McNerney (D-CA) and Bob Latta (R-OH) introduced H.R. 2931,the Enhancing Grid Security through Public-Private Partnerships Act, to permanently fund

public-private partnerships to promote and advance the physical and cybersecurity of electric utilities. The House Energy & Commerce Committee approved H.R. 2931 unanimously in June. APPA strongly supports the bill. There is not currently a standalone Senate companion, but a similar provision is included in a draft infrastructure bill by Senate Energy & Natural Resources Committee Chairman Joe Manchin (D-WV).

"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 that, if damaged, would have the most severe impacts on their ability to keep the lights 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 such exercise, GridEx V, took place in November 2019 and involved over 500 organizations and 7,000 participants from industry, government agencies, and partners in Canada and Mexico. APPA was significantly involved in the planning for GridEx V to further allow distribution utilities to get value from the distributed play portion of the exercise. One hundred public power organizations participated in the GridEx V distributed play, up from 53 that did so at GridEx IV in 2017. Managed by NERC and the E-ISAC, GridExV also included an executive tabletop exercise where 108 electric sector executives and senior U.S. government officials worked through incident response protocols to address widespread outages. GridEx events are conducted every two years; GridEx VI is scheduled for November 2021.

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 more than 170 entities across all segments of the industry, serving more than 80 percent of all U.S. electricity 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.

Administrative Action

Supply Chain Security Executive Actions

On May 1, 2020, President Trump signed an Executive Order 13920 (EO or order), *Securing the United States Bulk Power System,* deeming "the unrestricted foreign supply of bulk-power system electric equipment" as an "unusual and extraordinary threat to national security." The order broadly prohibited any person subject to federal jurisdiction from acquiring, importing, transferring, or installing bulk-power system electric equipment designed, developed, manufactured, or supplied by foreign adversaries when those transactions pose an undue or unacceptable risk to the grid or national security. DOE was tasked with leading a broad inter-agency effort to further define and implement the order's requirements within 150 days. As part of the implementation of the EO, on December 17, 2020, DOE released a prohibition order aimed at reducing the risks that entities associated with China pose to the nation's BPS. The order, which took effect January 16, 2021, prohibited utilities that supply critical defense facilities from procuring from China specific BPS equipment that poses an undue risk to the BPS, the security or resilience

of critical infrastructure, the economy, national security, or safety and security of Americans. The order only applied to utilities that have been designated as defense critical electric infrastructure (DCEI); a small number of public power utilities have been notified that they have been designated as DCEI.

On his first day in office, President Joe Biden signed an Executive Order, *Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis,* that included a provision suspending EO 13920 for 90 days and directing DOE and the Office of Management and Budget to "jointly consider whether to recommend that a replacement order be issued." On April 20, DOE announced that it was revoking the December 17, 2020, prohibition order on securing critical defense facilities [EO 13920 itself was briefly reinstated following the 90-day suspension, but the emergency declaration of the EO expired on May 1]. In conjunction with the announcement that it was revoking the prohibition order, DOE announced a new request for information (RFI), "Ensuring the Continued Security of the United States Critical Electric Infrastructure," seeking input from stakeholders to inform future recommendations for supply chain security in U.S. energy systems. APPA submitted comments in response to the RFI on June 7, asking DOE to focus on four foundational principles as it considers further action on energy sector supply chain security: (1) new measures must be risked-based; (2) directives should be clear, prospective, and scalable; (3) directives must be cost-conscious; and (4) DOE should focus on vendor risks.

NSC "100 Day Industrial Control Systems Cybersecurity Sprint"

On April 20, the Biden administration announced that it was launching a new initiative to enhance the cybersecurity of electric utilities' industrial control systems (ICS). This 100 day "sprint" is a coordinated effort between the National Security Council (NSC), DOE, and the ESCC to encourage and support utilities' visibility and situational awareness into their ICS and OT networks. APPA, as the primary public power point of contact for the initiative, is working with public power utilities to facilitate their participation in this voluntary pilot program. This effort has appropriately raised the issue of ICS security to a higher priority in the federal government. APPA views this sprint as the start of a long journey of collaboration between public power and the federal government, which includes the work being done through the CESER grant to APPA.

APPA Position

The regulations and standards ("NERC-FERC") process set up in EPAct05 provide a solid foundation for strengthening the industry's security posture. These mandatory standards evolve with input from subject-matter experts from across industry and government. However, the industry recognizes that it cannot protect all assets from all threats all the time, and instead must manage risk. APPA believes that close coordination among industry and government partners at all levels is imperative to deterring attacks and preparing for emergency situations.

APPA Contact

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

Jack Cashin, Director, Policy Analysis & Reliability Standards, 202-467-2979 / jcashin@publicpower.org

Nathan Mitchell, Senior Director, Operations Programs, 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.