AMERICAN PUBLIC POWER ASSOCIATION
80 Years of Powering Strong Communities

ISSUE BRIEF July 2020

Grid Security

Summary

The electric utility industry (including public power utilities) takes very seriously its responsibility to maintain a strong electric grid. It is the only critical infrastructure sector besides nuclear power that has mandatory and enforceable federal regulatory standards in place for cyber and physical security (collectively known as grid security). As the grid evolves, unfortunately, so do threats to its integrity. The threat of cyber-attacks is relatively new compared to long-known physical threats, but a cyberattack with operational consequences could occur and cause disruptions in the flow of power if malicious actors were able to hack into data systems used in some electric generation, transmission, and distribution infrastructure. The American Public Power Association (APPA) believes that the industry itself, with the North American Electric Reliability Corporation (NERC), has made great strides in addressing cybersecurity threats, vulnerabilities, and potential emergencies. Given the persistence 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.

Background and Congressional Action

The electric utility sector is the only critical infrastructure sector besides nuclear power plants (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). Under section 215, NERC working with electric industry experts, regional entities, and government representatives, drafts reliability, physical, and cyber security standards that apply across the North American grid, including Canada.[1] Participation by industry experts and compliance personnel in the NERC 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 conducts 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.

Cybersecurity

To date, the efforts of electric utilities to maintain a robust cybersecurity defense, along with the sector's Federal Power Act (FPA) section 215 processes, have prevented a successful cyberattack from causing operational consequences on the bulk electric system in the United States. That said, APPA has long recognized that increased information sharing and appropriately tailored liability protection would further enhance the industry's ability to guard against cyberattacks. As such, the association strongly supported passage of the Cybersecurity Act of 2015, which was incorporated as Division N of H.R. 2029, the Consolidated Appropriations Act, 2016. The act set up policies and procedures for sharing cybersecurity threat information between the federal government and private entities (which include public power) and between private entities and provides limited liability protection for these activities if conducted in accordance with the act.

In addition to the Cybersecurity Act of 2015, APPA strongly supported Section 61003 of P.L. 114-94 (the FAST Act), which codified the designation of the Department of Energy (DOE) as the Sector-Specific Agency for cybersecurity for the energy sector and gave the Secretary of Energy broader authority to address grid security emergencies under the FPA. A final rule entitled, "Grid Security Emergency Orders: Procedures for Issuance," was issued on January 10, 2018. APPA encourages DOE

1 NERC is the electric reliability organization for North America, subject to oversight by the Federal Energy Regulatory Commission; it develops and enforces reliability standards for the bulk power system. The Electricity Information Sharing and Analysis Center serves as the primary security communications channel for the electricity sector.

to use existing protocols and procedures to consult with industry prior to and during these emergencies. The new authority 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 and other sunshine laws. Specifically, the provision directed that FERC-designated CEII be exempt from disclosure for a period of up to five years with a process to lift the designation or challenge it in court and established sanctions for the unauthorized disclosure of shared information. FERC issued a final rule to implement this provision on December 21, 2016. APPA encourages FERC to follow the procedures to protect all utility operational data given to it in mandatory regulatory filings. Senators Lisa Murkowski (R-AK) and Jim Risch (R-ID) introduced a bill, S. 3688, the Energy Infrastructure Protection Act of 2020, on May 12, 2020, aimed at further strengthening protections for CEII. APPA appreciates the senators' efforts in this issue area and hopes the Energy & Natural Resources Committee considers the legislation this fall.

Physical Security

NERC has considered proposals and issued regularly updated security guidelines to enhance the physical security of assets in the bulk electric system. In response to developing threat analyses in March 2014, FERC used its authority under FPA section 215 to direct NERC to submit within 90 days proposed reliability standards requiring utilities with critical assets to take steps to address physical security vulnerabilities. NERC submitted a draft standard, known as CIP-014, to FERC in 77 days, which FERC subsequently approved.

The nation's electric distribution systems have always been, and are today, regulated by state and local governments. This is a deliberate separation of power given the retail nature of distribution systems, and the vast differences in the configuration, size, and ownership of the 3,000 distribution utilities in the U.S. Because of this diversity among distribution systems, each individual utility's role in the security of its distribution facilities is paramount. While APPA supports physical security standards at the bulk electric system, it does not support a federally legislated "one-size-fits-all" mandate on the distribution level due to the differences in systems and regions noted above.

Administrative Action

On May 1, 2020, President Trump signed an Executive Order (EO or order) on Securing the United States Bulk-Power System. The EO deems "the unrestricted foreign supply of bulk-power system electric equipment" as an "unusual and extraordinary threat to national security." The order broadly prohibits 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 is tasked with leading a broad inter-agency effort to further define and implement the order's requirements within 150 days. The department is also authorized to publish criteria for recognizing bulk-power system equipment and vendors as "pre-qualified." NERC is preparing an alert in conjunction with the EO that seeks to gather extent-of-condition information in order to better estimate the risk of installed BPS electric equipment manufactured or supplied by certain foreign entities of concern. A Request for Information to industry (RFI) was issued on July 8, 2020, ahead of the expected release of a Notice of Proposed Rulemaking (NOPR) this fall. APPA will be responding to the RFI and NOPR.

Industry Action

Outside of the legislative process, APPA and its members, as well as other utilities, continue to participate in the NERC Critical Infrastructure Protection (CIP) standards drafting process on cyber and physical security. As attacks on critical electric infrastructure are ever-changing, so must be the nature of the industry's defenses, which is why the CIP standards are regularly updated. For example, in June 2019, FERC approved an updated version of a standard for cyber security incident reports. The revised standard broadens the reporting obligations to require "reporting of cyber security incidents that either compromise or attempt to compromise" certain electronic systems. More recently, in June 2020, FERC issued a Notice of Inquiry (NOI) seeking comments on whether CIP reliability standards adequately address cybersecurity risks pertaining to data security, detection of anomalies and events, and mitigation of cybersecurity events in comparison to the National Institute of Standards Technology (NIST) Cybersecurity Framework. In addition, the NOI seeks comment on the potential risk of a coordinated cyberattack on geographically distributed targets and whether FERC action, including potential modifications to the CIP reliability standards, would be appropriate to mitigate such risk. APPA is reviewing the NOI and will file comments.

APPA recognizes that robust grid security means more than mandatory CIP standards, which is why it is also involved with internal and external working groups to enhance the security of the electric grid. The association and its members play a leadership role on the Electricity Subsector Coordinating Council (ESCC), one of the coordinating councils established in the National Infrastructure Protection Plan to facilitate ongoing communication between the sector (or subsector) and its sector-specific federal agency, which in the case of the ESCC is DOE. The ESCC provides senior industry and government officials

with a venue to coordinate sector-wide policies and initiatives to improve cyber and physical security and emergency preparedness. Through the ESCC, APPA works with the other critical infrastructure sectors, such as the telecommunications and finance sectors. The full ESCC meets twice a year and its issue-specific subgroups communicate on a regular basis.

Regardless of the cause of damage to the electric system, preparations to ensure mitigation, response, and restoration are the same: grid operators prioritize risk to enhance protection around critical assets, engineer redundancy to avoid single points of failure, stockpile spare equipment for hard-to-replace components, and develop other contingencies to minimize impacts. The ESCC is involved in all aspects of these preparations.

- **Exercises**
  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 Electricity Information Sharing and Analysis Center, GridEx V 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.

- **Mutual Assistance Programs**
  The three 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 emergencies. In October 2019, APPA held the 2019 Public Power Mutual Aid Exercise in Syracuse, NY. This event was a functional tabletop exercise that included a category 5 hurricane impacting the U.S. Virgin Islands, Puerto Rico, and the southeast and northeast regions of the U.S. The exercise tested the capabilities of the mutual aid network, inter-organization and inter-agency coordination, and the tools and technologies currently used to support mutual aid coordination.

  The exercise was made possible with funds provided by a five-year cooperative agreement with DOE's Infrastructure Security and Energy Restoration Division. Under the agreement, APPA is entitled to receive up to $200,000 a year to fund disaster response exercises and preparedness. This is the fifth budget year of the agreement; however, due to the COVID-19 pandemic, DOE has granted APPA a one-year extension.

- **Spare Equipment Programs**
  Electric utilities regularly share transformers and other equipment through long existing bi- and multi-lateral 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.

In addition, APPA has partnered directly with DOE, signing a three-year cooperative agreement in 2016 for up to $2.5 million per year to accelerate the association's efforts to help its members understand and implement resiliency, cybersecurity, and cyber-physical solutions, including refining and improving the adoption of advanced control concepts. Among other programs, this grant led to the development of a cybersecurity scorecard for public power utilities to assess their cyber readiness (328 utilities have completed the scorecard thus far), 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. In a report accompanying the Further Consolidated Appropriations Act, 2020 (H.R. 1865), Congress directed DOE to fund the program at $3 million for another year. Legislation based on the success of this program that would seek to permanently fund public-private partnerships to promote and advance the physical and cybersecurity of electric utilities, H.R. 359, the Enhancing Grid Security through Public-Private Partnerships Act, was approved by the House Energy & Commerce Committee in October 2019. H.R. 359 is sponsored by Representatives Bob Latta (R-OH) and Jerry McNerney (D-CA). Senators Cory Gardner (R-CO) and Michael Bennet (D-CO) sponsored a companion bill, S. 2095, which was approved by the Senate Energy & Natural Resources Committee in October 2019. The bill was also incorporated into the large bipartisan energy package, S. 2657, the American Energy Innovation Act (AEIA), that stalled on the Senate floor in March. APPA strongly supports H.R. 359 and S. 2095.

American Public Power Association Position

The regulations and standards ("NERC-FERC") process set up in EPAct05 continues to 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 and, as such, will continue to invest considerable resources into this effort.

The association supports the adoption by public power utilities of appropriate physical-security measures that consider the specific assets being secured. APPA also supports enhanced dialogue between the industry and federal government on physical-security threats and potential remediation, but does not support federal mandates in this area at the distribution level because a one-size-fits-all approach would do little to secure those assets.

American Public Power Association Contacts

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

Nathan Mitchell, Senior Director, Cyber & Physical Security Services, 202-467-2925 / nmitchell@publicpower.org

Sam Rozenberg, Engineering Services Security Director, 202-467-2985 / srozenberg@publicpower.org

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