AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

ISSUE BRIEF July 2019

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 overlays used in some electric generation, transmission, and distribution infrastructure. While the American Public Power Association (APPA or Association) 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, 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, 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 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.

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 section 215 of the Federal Power Act 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 power 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 11, 2017, President Trump signed an executive order (EO) entitled, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," and directed DOE, along with government and industry stakeholders, to assess the potential scope and duration of a prolonged power outage caused by a cyber attack and the readiness of the U.S. to manage such an incident. The report, issued in response to the EO on May 30, 2018, summarized its findings: "While it was found that no lasting damage—physical, cyber-physical, or otherwise—has been observed from the cyberattacks and intrusions targeting U.S. electric utilities that have been reported to date, there are key trends that are increasing the risk of significant cyber incidents." The report found that "existing capability gaps fall largely into seven main categories: cyber situational awareness and incident impact analysis; roles and responsibilities under cyber response frameworks; cybersecurity integration into state energy assurance planning; electric cybersecurity workforce and expertise; supply chain and trusted partners; public-private cybersecurity information sharing; and resources for national cybersecurity preparedness."

President Trump's EO built on the one issued by President Obama in February 2013 requiring the creation of a cybersecurity framework, which was subsequently released by the National Institute for Science and Technology in February 2014. APPA has strongly encouraged its members to adopt this framework and evaluate their cybersecurity plans.

DOE and the Department of Homeland Security (DHS) reorganized some offices and efforts in 2018 to better address cybersecurity threats confronting the nation. In February 2018, Secretary of Energy Rick Perry announced the establishment of a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at DOE to focus on "energy infrastructure security and support the expanded national security responsibilities assigned to DOE." Karen Evans was confirmed to head the new office on August 28, 2018. In July 2018, then DHS Secretary Kristin Nielsen announced the creation of the National Risk Management Center (NRMC). Lead by Director Robert Kolasky, the NRMC is pursuing a strategic approach to defending all critical infrastructure sectors by focusing on vulnerabilities arising out of the interconnectedness of the sectors. On April 30, 2019, NRMC released a list of 55 critical functions, "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." For electricity, the critical functions are generation, transmission, and distribution of electricity. The list was developed in consultation with the critical infrastructure sectors and will guide further work to understand cross-sector dependencies and what resources are needed to restore critical functions after a major event.

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.

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, which meets three times a year, 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.

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 IV, took place in November 2017 and involved over 450 organizations and 6,500 participants from industry, government agencies, and partners in Canada and Mexico. Managed by NERC and the Electricity Information Sharing and Analysis Center, GridEx IV also included an executive tabletop exercise where 32 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. An after-action report from GridEx IV was released in March 2018. The next GridEx will take place November 13-14, 2019.

- **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. The years of experience industry has had in deploying these resources is a valuable tool. In October 2018, APPA hosted an exercise intended to test the use of mutual aid in a California flooding event. The scenario involved an atmospheric river event in the state where rains flooded much of the Central Valley, including the cities of Sacramento, Stockton, and Modesto. In addition, the Los Angeles area suffered damage from 200- to 500-year flooding levels and windstorms. This 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 $250,000 a year to fund disaster response exercises and preparedness. This is the fourth budget year of the agreement.

- **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 (256 have completed the scorecard thus far), funded 15 tabletop exercises across the country in 2017, and 15 trainings in 2018. Legislation based on the success of this program, H.R. 5240, the Enhancing Grid Security through Public-Private Partnerships Act, was approved by the House Energy & Commerce Committee in June 2018. Sponsored by Representatives Bob Latta (R-OH) and Jerry McNerney (D-CA), the bill would establish a permanent program at DOE to facilitate and encourage public-private partnerships to promote and advance physical and cybersecurity of electric utilities. APPA supported the bill, which unfortunately was not considered in the Senate. This legislation was reintroduced in January 2019 as H.R. 359 and approved by the House Energy & Commerce Committee's Subcommittee on Energy on May 16. Senators Cory Gardner (R-CO) and Michael Bennet (D-CO) introduced a companion bill in the Senate on July 11.

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

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.