AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

ISSUE BRIEF June 2017

Physical Security and the Electric Sector

Summary

While threats from cyber attackers are on the rise, public power utilities also face threats to their physical infrastructure—the poles, wires, substations, transformers, and generating facilities comprising these utilities' means of delivering electricity to their customers. The majority of physical-security threats to electric infrastructure, such as copper theft, have been known for years. However, more sophisticated threats have emerged with the attack on a California substation in April 2013. While customers did not lose power as a result of the attack due to the redundancy built into the system, it was a reminder to law enforcement and electric utilities about the importance of working together to protect critical utility assets.

Electric utilities, including public power utilities, take physical (and cyber, as discussed in the companion issue brief "Cybersecurity and the Electric Sector") threats seriously and employ risk management programs to prioritize facilities and equipment, develop contingency plans, and employ defense-in-depth techniques to "keep the lights on."

Background

Public power utilities intimately understand the importance of physical security and have longstanding programs and protocols designed to protect their utility systems. As the nature of physical threats has changed over the years, public power utilities have planned, prepared, and responded accordingly. Today, due to security breaches, such as vandalism and terrorist attacks that can cause damage to this infrastructure, utilities must develop the best available mitigation practices to address such attacks. Physical infrastructure security can range from a substation with cameras, locks, and fences to engineering new facilities utilizing design bases threat methodology.

In recent years, a few high profile incidents of physical security failure have drawn increased scrutiny from several areas. One incident that received press attention was a shooting incident at a transformer at an Arkansas utility. Another high profile incident took place at the Metcalf substation on Pacific Gas and Electric's (PG&E) system in California where at least one person fired over 150 rounds of ammunition and cut two critical telecommunications cables to the substation. These and several other press reports on attacks on utility infrastructure have caused some Members of Congress to react by introducing or exploring legislation related to utility security.

Congressional and Regulatory Action

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. Given this situation, each individual utility's role in the security of its distribution facilities is paramount. However, in the past few Congresses, several legislative proposals have included physical-security requirements for electric utilities. While the American Public Power Association (Association or APPA) supports physical security initiatives at the bulk power system and distribution levels, we do not support a federally legislated "one-size-fits-all" mandate due to the differences in systems and regions noted above.

The North American Electric Reliability Corporation (NERC), which promulgates mandatory and enforceable standards for the federally jurisdictional bulk power system to ensure the reliability of that system, has considered proposals and issued regularly updated security guidelines that would enhance physical-security requirements related to access to cyber assets at electric utilities.[1] In response to developing threat analysis in March 2014, the Federal Energy Regulatory Commission (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 submit-

[1] (See APPA's "Electric Transmission Policies" issue brief for additional information on the bulk power system.)

ted a draft standard, known as CIP-014, to FERC in 77 days, which FERC subsequently approved.[2]

Industry Action

APPA and its members continually seek to promote increased physical security in a variety of manners and forums. Most notably, the Association and its members are intimately involved in the Electric Subsector Coordinating Council (ESCC), one of the coordinating councils established in the National Infrastructure Protection Plan (NIPP) to facilitate ongoing communication between the sector (or subsector) and its sector-specific federal agency, which in the case of the ESCC is the Department of Energy (DOE). The ESCC, which meets three times a year, is a venue for senior industry and government officials to coordinate sector-wide policies and initiatives to improve cyber and physical security and emergency preparedness.

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 our ability to provide electricity. The industry participates in many incident response exercises, including five national-level exercises since November 2015. One such exercise, GridEx III, involved more than 360 organizations and 4,400 participants from industry, government agencies, and partners in Canada and Mexico. Managed by the North American Energy Reliability Corporation (NERC) and the Electricity Information and Analysis Center (E-ISAC), GridEX III 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.[3] GridEx events are conducted every two years; GridEx IV is planned for November 2017.

- **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 2016, APPA hosted an exercise intended to review, validate, and examine gaps in the Public Power Mutual Aid Playbook (MAP), in a scenario of significant physical damage caused by an earthquake in the New Madrid Seismic Zone. This tabletop exercise was funded in part by a grant awarded to APPA by DOE.

- **Spare Equipment Programs**
  Electric companies 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 (STEP), SpareConnect, and the newly formed Grid Assurance program—to improve grid resiliency.

American Public Power Association Position

The Association supports the adoption by public power utilities of appropriate physical-security measures that take into account 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. In addition, the Association supports the FERC/NERC relationship codified in FPA Section 215 and as used to craft a standard on electric utility physical security for the bulk-power system.

American Public Power Association Contacts

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

Cory Toth, Government Relations Director, 202-467-2939 / ctoth@publicpower.org

Nathan Mitchell, Sr. Director, Electric Reliability Standards and Security, 202-467-2925 / nmitchell@publicpower.org

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

[2] See APPA's "Cybersecurity and the Electric Sector" issue brief for more information about the FERC/NERC relationship, as codified in FPA Section 215.

[3] NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC); it develops and enforces reliability standards for the bulk power system. The E-ISAC serves as the primary security communications channel for the electricity sector.