Congressional Research Service
Informing the legislative debate since 1914

NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?

-name redacted-
Specialist in Energy and Infrastructure Policy

Updated March 19, 2018

Congressional Research Service
7-....
www.crs.gov
R45135

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

A 2013 rifle attack on a critical electric power substation in Metcalf, CA, marked a turning point for the U.S. electric power sector. The attack prompted utilities across the country to reevaluate and restructure their physical security programs. It also set in motion proceedings in Congress and at the Federal Energy Regulatory Commission (FERC) which resulted in a new mandatory *Physical Security Reliability Standard* (CIP-014) for bulk power asset owners promulgated by the North American Electric Reliability Corporation (NERC) in 2015. In the three years since FERC approved this new standard, security risks to the power grid have become an even greater concern in the electric utility industry. Reflecting these ongoing security concerns, legislative proposals in the 115th Congress include provisions directed at power grid physical security. Congress also continues its oversight of grid security and implementation of NERC's security standards.

Three entities play key roles in standards oversight and support of implementation for bulk power physical security. NERC and FERC oversee implementation of the CIP-014 standards, while the Department of Energy plays a supporting role in helping bulk power asset owners to protect their critical infrastructure. The detailed findings of NERC's compliance activities are not publicly disclosed due to their confidential nature. However, NERC has stated that the utility industry is making progress towards effective implementation of the CIP-014 standard and NERC has been "encouraged" by grid security measures put in place so far. NERC compliance audits as of February 2018 have uncovered no major failures to date.

In addition to compliance with NERC's standards, there have been other observable changes within the electricity sector reflecting greater emphasis on bulk power physical security. These changes include realignment in corporate structure to support physical security, incorporating physical security in transmission planning, new security products and services, utility capital investment in physical security, and utility participation in voluntary security programs. While public information about such changes is limited, it suggests they may be significant and widespread.

Although the electric power sector seems to be moving in the overall direction of greater physical security for critical assets, many measures have yet to be implemented and the process of corporate realignment around physical security is still underway. NERC's CIP-014 standards have been promulgated recently, and bulk power asset owners have largely begun enhancing physical security under the standard over the last two years. Therefore, although it is probably accurate to conclude that, based on the objectives of the CIP-014 standards, the U.S. electric grid is more physically secure than it was five years ago, it has not necessarily reached the level of physical security needed based on the sector's own assessments of risk. Bulk power security remains a work in progress.

Congress continues to be concerned about the current state of electric grid physical security. Among many specific issues of potential interest, Congress may focus on several with policy significance: security implementation oversight, cost recovery, hardening vs. resilience, and the quality of threat information. As CIP-014 implementation and other physical security initiatives proceed, Congress also may seek to maintain its focus on the power sector's overall progress, not only on short term compliance with NERC's security standards, but also on structural changes supporting physical security as a priority far into the future.

Contents

Introduction 1
Power Grid Threat Environment 2
NERC's Physical Security Standards 3
    Physical Security Standard Requirements 4
Federal Oversight and Support 5
    NERC's Implementation Oversight 5
        Electricity Information Sharing and Analysis Center 7
    FERC Oversight 7
    DOE Initiatives 8
Observed Changes in Bulk Power Physical Security 9
    Corporate Structure Supporting Physical Security 9
    Physical Security in Long-Term Transmission Planning 11
    New Security Products and Services 12
    Capital Investment in Physical Security 13
    Utility Participation in Voluntary Security Programs 14
        NERC Grid Security Exercises 14
        DHS Critical Infrastructure Surveys 15
Legislative Proposals in the 115th Congress 15
Policy Issues for Congress 16
    Oversight of Physical Security Implementation 17
    Financial Requirements and Cost Recovery 18
    Hardening vs. Resilience 19
    Threat Information 19
Conclusion 20

Contacts

Author Contact Information 21

Introduction

Securing the electric power grid is among the highest priorities for critical infrastructure protection in the United States. In the past, power grid facilities have had varying degrees of access control and surveillance depending upon the facility type and location. These measures were largely focused on public safety (reflecting liability concerns) and preventing vandalism and theft. More recently, federal agencies, Congress, and the utility industry have focused greater attention on the vulnerability of the power grid, especially the high voltage transmission (bulk power) system, to terrorist attacks which could cause widespread, extended blackouts.

Until 2013, the emphasis of analysts and policymakers was on power grid cybersecurity—protecting the computer controls and communication systems used to operate the grid. However, a 2013 rifle attack on an electric transmission substation in Metcalf, CA, shifted more attention to the physical security of power grid critical assets. In response to the Metcalf attack, as well as other grid incidents and findings from utility security exercises, Congress passed new legislation to strengthen power grid physical security and to facilitate recovery in the event of a successful attack.[1] Congress also sought stronger physical security standards from the Federal Energy Regulatory Commission (FERC) under the commission's existing statutory authority to regulate the reliability of the bulk power system. FERC, in turn, ordered the North American Electric Reliability Corporation (NERC)—the not-for-profit organization responsible for ensuring grid reliability—to promulgate new requirements for the physical security of bulk power critical infrastructure.[2] After consultation within the utility industry, NERC proposed new physical security standards in May 2014. FERC approved them, with minor changes, the following November.[3]

Since 2014, security risks to the power grid have become an even greater concern in the electric utility industry. Addressing them has remained a concern of Congress.[4] An emphasis on physical risk to the power grid was underscored in September 2016 by another successful rifle attack on a transformer substation—in Utah. Reflecting ongoing security concerns, legislative proposals in the 115th Congress include provisions directed at power grid physical security. Congress also continues its oversight of FERC's grid security activities and the implementation of NERC's physical security standards.

This report examines changes to the physical security of the electric power grid since the promulgation of NERC's physical security standards. The report discusses the current risk environment for the bulk power system. It summarizes the key requirements of NERC's security standards, including its applicability to specific assets, implementation deadlines, and oversight. The report reviews observable changes in the utility sector related to physical security. It concludes with an overview of proposed legislation and a discussion of policy issues for Congress.

[1] The Fixing America's Surface Transportation (FAST) Act (P.L. 114-94), which became law on December 4, 2015, contains provisions to protect or restore the reliability of critical electric infrastructure or defense of critical electric infrastructure during a grid security emergency (§1104).

[2] Among other functions, NERC develops and enforces reliability standards, monitors the grid, and trains industry personnel. In the United States, NERC is subject to Federal Energy Regulatory Commission oversight

[3] For more historical background and details regarding the development of NERC's standards, see CRS Report R43604, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, by (name redacted) .

[4] See, for example, Senator Ron Johnson, Chairman, Opening statement before the Senate Committee on Homeland Security and Governmental Affairs hearing on "Threats to the Homeland," September 27, 2017.

This report focuses primarily on physical security efforts to prevent successful physical attacks on the bulk power system. For analysis of issues specifically related to power grid cyberattacks and cybersecurity, see CRS Report R43989, *Cybersecurity Issues for the Bulk Power System*, by (name redacted) . This report also does not address issues related to security incident recovery or restoration, except in the context of preventive physical security.

Power Grid Threat Environment

Grid security analysts and policymakers have long been aware of physical risks to bulk power critical infrastructure, especially to high voltage (HV) transformer stations and substations, which serve as key nodes within the electric transmission system.[5] The 2013 Metcalf attack, in which an unknown perpetrator firing a .30 caliber rifle disabled a critical 500 kilovolt (kV) transformer substation, demonstrated that such facilities face real and potentially sophisticated threats.[6] The September 2016 rifle attack on a 69 kV transformer substation in Utah—which reportedly left 13,000 rural customers without power for up to eight hours—showed that similar incidents could occur almost anywhere on the grid.[7] A successful cyberattack on Ukraine's power grid in 2015, which was reportedly attributed to Russian hackers, showed that foreign entities could view power grids as attractive targets.[8] A 2017 report from the National Academy of Sciences concludes: "While to date there have been only minor attacks on the power system in the United States, large-scale physical destruction of key parts of the power system by terrorists is a real danger. Some physical attacks could cause disruption in system operations that last for weeks or months."[9]

The persistent threat environment has been changing the perception of physical threats among power grid owners and operators. For example, surveys of electric utility employees show that their physical (and cyber) security concerns are growing.[10] Exelon Corporation, one of the nation's largest utility holding companies, stated in its 2016 annual report

> Threat sources continue to seek to exploit potential vulnerabilities in the electric…utility industry associated with protection of sensitive and confidential information, grid infrastructure and other energy infrastructures, and such attacks and disruptions, both physical and cyber, are becoming increasingly sophisticated and dynamic.…The risk of these system-related events and security breaches occurring continues to intensify.…[11]

[5] See, for example, National Research Council, *Terrorism and the Electric Power Delivery System*, 2012 and Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453, June 1990.

[6] RTO Insider, "Substation Saboteurs 'No Amateurs,'" April 2, 2014, http://www.rtoinsider.com/pjm-grid2020-1113-03/.

[7] Pat Reavy, "Power Company Offers Rare $50K Reward for Information on Vandalism," *Deseret News*, September 29, 2016. A substation rated at 69 kilovolts is not considered a "high voltage" transmission asset, although it may still serve large numbers of customers.

[8] Jim Finkle, "U.S. Firm Blames Russian 'Sandworm' Hackers for Ukraine Outage," *Reuters*, January 7, 2016. The attack reportedly cut power to 80,000 customers for about six hours.

[9] National Academy of Sciences, Engineering, and Medicine, *Enhancing the Resilience of the Nation's Electricity System*, 2017, p. 65, https://doi.org/10.17226/24836.

[10] Utility DIVE, *2017 State of the Electric Utility Survey*, April 10, 2017, https://s3.amazonaws.com/dive_assets/rlpsys/SEU_2017.pdf.

[11] Exelon Corporation, *Annual Report Pursuant to Section 13 or 15(d) of the Securities and Exchange Act of 1934 for the Fiscal Year Ended December 31, 2016*, Form 10-K, February 13, 2017, p. 63.

Xcel Energy, another major utility owner, likewise states in its 2016 annual report

> Our generation plants, fuel storage facilities, transmission and distribution facilities and information systems may be targets of terrorist activities… The potential for terrorism has subjected our operations to increased risks and could have a material effect on our business.[12]

Accordingly, electricity sector-wide security exercises conducted by NERC have simulated attacks on power grid critical assets combining both cyber and physical dimensions.[13] These exercises are further discussed later in this report.

NERC's Physical Security Standards

On March 7, 2014, FERC ordered NERC to submit proposed reliability standards requiring transmission owners meeting certain criteria "to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation" of the power grid.[14] In its order FERC stated that physical security standards were necessary because "the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks."[15] According to the FERC order, the new reliability standards were to require transmission owners or operators to perform a risk assessment of their systems to identify "critical facilities," evaluate the potential threats and vulnerabilities to those identified facilities, and develop and implement a security plan designed to protect against physical attacks on those identified critical facilities.[16] The order required that each of these steps be verified by NERC or another third party qualified to review them.

On May 23, 2014, NERC filed with FERC its proposal for mandatory physical security standards.[17] On November 20, 2014, FERC approved the proposed standard, with minor changes, as NERC's new *Physical Security Reliability Standard* (CIP-014-1).[18] Following publication in the *Federal Register*, FERC's order approving the standard became effective on January 26, 2015.[19] FERC approved a revised version of the standard (CIP-014-2) on July 14, 2015.[20]

---

[12] Excel Energy, Inc. *Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Fiscal Year Ended December 31, 2016*, Form 10-K, p. 44.

[13] North American Electric Reliability Corporation (NERC), *Grid Security Exercise (GridEx II): After-Action Report*, March 2014 and *Grid Security Exercise, GridEx III Report*, March 2016; Scott Heffentrager, PJM Interconnection, "GridEx IV Summary," slide presentation, November 27, 2017, http://www.pjm.com/-/media/committees-groups/committees/mc/20171127-webinar/20171127-item-04-2017-gridex-iv-summary.ashx.

[14] Federal Energy Regulatory Commission (hereinafter, FERC), *Reliability Standards for Physical Security Measures*, Order Directing Filing of Standards, Docket No. RD14-6-000, March 7, 2014, p.1, http://www.ferc.gov/CalendarFiles/20140307185442-RD14-6-000.pdf.

[15] FERC, March 7, 2014, p. 2.

[16] FERC, March 7, 2014, pp. 3-4.

[17] NERC, Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-014-1, May 23, 2014, http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Physical%20Security%20CIP-014-1.pdf.

[18] FERC, "Physical Security Reliability Standard," Docket No. RM14-15-000, Order No. 802, November 20, 2014.

[19] NERC, "Physical Security Reliability Standard Implementation," January 16, 2015, https://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20(Agenda%20Excerpt).pdf.

[20] FERC, letter order to the North American Electric Reliability Corporation, Docket No. RD-15-4-000, July 14, 2015, http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Letter_Order_CIP-014_20150714_RD15-4.pdf.

Required compliance for the standard began on October 1, 2015 with completion of the final parts required by November 24, 2016 for all applicable entities.

Physical Security Standard Requirements

The stated purpose of NERC's physical security reliability standard is "to identify and protect transmission stations and transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or cascading within an interconnection."[21] It applies to transmission owners with assets operating at 500 kV or higher as well as owners with substations operating between 200 kV and 499 kV if they meet certain interconnection or load-carrying criteria.[22] The standard, generally referred to as "CIP-014," consists of six principal requirements (R1-R6), summarized as follows:

R1. Risk assessments by transmission owners to identify critical transmission facilities;

R2. Independent third party verification of risk assessments conducted under R1;

R3. Requirement for transmission owners with critical facilities identified under R1 but not under their operational control to notify the transmission operator of these facilities;[23]

R4. Mandatory threat and vulnerability assessments for critical facilities conducted by transmission owners and operators;

R5. Development, documentation, and implementation of physical security plans to protect critical facilities; and

R6. Independent third party review of the threat and vulnerability assessments performed under R4 and security plans developed under R5.[24]

The standard also lays out a process for compliance monitoring and assessment including audits, self-certifications, spot checking, violation investigations, self-reporting, and handling complaints.[25] The new standard is enforced by NERC or another Regional Entity under a penalty review policy for mandatory reliability standards approved by FERC subject to the Commission's enforcement authority and oversight under the Energy Policy Act of 2005 (P.L. 109-58).[26] Monitoring of compliance with the standard is further discussed below.

[21] NERC, *CIP-014-2 – Physical Security*, printed December 5, 2017, p. 1, available at http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=Physical%20Security&jurisdiction=United%20States. (Hereinafter CIP-014-2). This report uses the terms "critical assets" and "critical substations" to mean "critical transmission stations and transmission substations" as defined under the CIP-014 standard.

[22] CIP-014-2.

[23] A regional transmission operator (RTO) administers the transmission grid for multiple transmission owners in a specified region in accordance with FERC Order No. 2000. RTOs and independent system operators (ISOs) are defined in Section 3 of the Federal Power Act (16 U.S.C. 796).

[24] CIP-014-2, pp. 3-6.

[25] CIP-014-2, p. 8.

[26] FERC, *Statement of Administrative Policy on Processing Reliability Notices of Penalty and Order Revising Statement in Order No. 672*, Docket Nos. AD08-6-000 and RM05-30-002, April 17, 2008.

Federal Oversight and Support

Three entities play key roles in standards oversight and implementation support for bulk power physical security. NERC and FERC directly oversee implementation of the CIP-014 standards, while the Department of Energy (DOE) plays a supporting role in helping bulk power asset owners to protect their critical assets.

NERC's Implementation Oversight

As stated above, with oversight by FERC, NERC has the authority to develop, oversee, and enforce implementation of the CIP-014 physical security standard.[27] NERC carries out these functions together with the eight Regional Entities (e.g., Midwest Reliability Organization) with which NERC has agreements to delegate its authority to monitor and enforce reliability standards compliance.[28] Collectively, NERC and the Regional Entities comprise the Electric Reliability Organization (ERO) Enterprise.

In general, NERC employs a risk-based framework to monitor compliance of all its grid reliability standards on the belief that monitoring and enforcement must be "right-sized" based on considerations including risk factors and management practices related to detecting, assessing, mitigating, and reporting of noncompliance.[29]

> As reliability risk is not the same for all registered entities, the Framework examines [bulk power system] risk of registered entities both collectively and individually, to determine the most appropriate [Compliance Monitoring and Enforcement Program] tool to use when monitoring a registered entity's compliance with NERC Reliability Standards. The Framework also promotes an examination into how registered entities operate and tailor compliance monitoring focus to areas that pose the greatest risk to [bulk power system] reliability.[30]

NERC's approach offers flexibility in both the frequency and type of compliance monitoring (e.g., offsite or onsite audits, spot checks, or self-certifications) applied to an entity under a particular standard based on its particular level of reliability risk.[31] To support its compliance approach, NERC may conduct various activities, such as publishing guidance documents, providing training, and conducting outreach, "to promote transparency and confidence" in the utility industry's implementation of a standard.[32]

In monitoring compliance of the CIP-014 standard, NERC's focus in 2015 and 2016 was on the standards' requirements to identify critical transmission stations and substations (Requirements

[27] NERC's authorities to monitor compliance with its reliability standards and impose financial penalties are found in FERC regulations at 18 C.F.R. 39.7.

[28] See NERC, "Key Players," web page, March 13, 2018, http://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx.

[29] NERC, *Overview of the ERO Enterprise's Risk-Based Compliance Monitoring and Enforcement Program*, September 5, 2014, p. iv.

[30] NERC, *2017 ERO Enterprise Compliance Monitoring and Enforcement Implementation Plan, Version 2.5*, May 2017, p. 3.

[31] NERC, May 2017, p. 3.

[32] NERC, "Physical Security Reliability Standard Implementation," January 16, 2015, p. 3, https://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Summary%20for%20January%2016%202015%20MRC%20Informational%20Session%20(Agenda%20Excerpt).pdf.

R1 and R2), ensuring that this identification was "appropriate and risk-informed."[33] NERC required covered entities to self-certify with respect to: risk-assessment, identifying critical assets, and third party verification. NERC also conducted voluntary outreach through on-site visits with 19 covered entities to discuss security measures and CIP-014 implementation challenges.[34] In cases where there have been discrepancies between utility-generated critical asset lists and critical assets identified by the independent third parties, NERC has required the covered entities to provide further information and explanation to address the discrepancy. NERC has also been conducting audits of entities which have identified more, or fewer, critical substations as a percentage of all their substations than is typical.[35] The detailed findings of NERC's compliance activities are not publically disclosed due to the confidential nature of security information. However, NERC stated that, based on observations in 2016, the utility industry was "making progress towards effective implementation of and compliance with CIP-014-2."[36] A NERC presentation about its voluntary and informal site visits reported "remarkable progress" on physical security among 19 asset owners visited as of February 2016.[37]

In 2017, NERC increased its focus on the scope of utility security plans (R5), including their timelines for implementing security measures and the utility industry's overall progress in implementing CIP-014. The ERO Enterprise has prioritized auditing the quality of covered entities' risk management plans. In the second quarter of 2017, compliance audit staff were provided with guidance and training on bulk power physical security best practices as a reference for evaluating the physical security measures implemented by the covered entities.[38]

The ERO Enterprise expects to complete audits of the largest entities within three years of the effective date of CIP-014. As of February 2018, NERC had conducted compliance audits of approximately 45% of the covered entities with critical transmission stations and substations as defined under CIP-014. NERC had also audited over 30% of entities that did not identify critical assets after applying the CIP-014 criteria (under R1). NERC staff expects to have audited approximately 70% of the entities with CIP-014 critical assets by the end of 2018.[39] According to its stated schedule, NERC would audit the remaining entities in 2019. Subsequent monitoring and enforcement will focus more heavily on implementation of measures in the grid security plans.

According to NERC, the audits completed to date have not uncovered any major compliance failures, and NERC has been "encouraged" by security measures that utilities have put in place so far.[40] NERC has found no serious risk violations of the CIP-014 standard. Of 19 noncompliance

[33] NERC, May 2017, p. 16.

[34] NERC, *2016 ERO Enterprise Compliance Monitoring and Enforcement Program Annual Report*, February 8, 2017, p. 18, http://www.nerc.com/pa/comp/CE/Compliance%20Violation%20Statistics/2016%20Annual%20CMEP%20Report.pdf.

[35] NERC, Staff meeting with CRS analysts, Washington, DC, December 7, 2017.

[36] NERC, May 2017, p. 16.

[37] Carl Herron, NERC, "CIP-014-02 Physical Security Site Visits," slide presentation, April 14, 2016, https://www.frcc.com/Compliance/EducationalMaterials/Educational%20Materials/Workshops%20-%20Workshop%20Event%20Materials/2016-04%20-%20OP%20Spring%20Compliance%20Workshop%20(April%2012-14)/7.%20CIP-014-2%20Physical%20Security%20Site%20Visits.pdf.

[38] NERC, *Compliance Monitoring and Enforcement Program Quarterly Report, Q2 2017*, August 9, 2017, p. 8, http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/Compliance%20Committee%20Open%20Meeting%20-%20August%209%202017.pdf.

[39] NERC, email to CRS, February 14, 2018.

[40] NERC, December 7, 2017.

issues identified, 8 were found to be "minimal" or "moderate" risk, with 2 warranting a financial penalty. The remaining 11 noncompliance issues are under review.[41]

Electricity Information Sharing and Analysis Center

In addition to its standards activities, NERC also supports security of the electric power sector as the operator of the Electricity Information Sharing and Analysis Center (E-ISAC). Established in 1998, the E-ISAC is the electricity sector's primary communications channel for security-related information, situational awareness, incident management, and coordination.[42] Among its key responsibilities, the E-ISAC gathers and analyzes security data, shares it with stakeholders, and communicates security risk mitigation strategies.[43] Bulk power entities are required to report physical security events to the E-ISAC under NERC's Event Reporting Reliability Standard (EOP-004), which was approved by FERC in 2013 and revised in 2015.[44]

Although operated by NERC, the E-ISAC is independent and organizationally separate from NERC's standards enforcement functions; information shared by utilities with the E-ISAC is not passed on to NERC compliance staff.[45] Nonetheless, the E-ISAC has played a role in facilitating industry understanding of physical security best practices. For example, the E-ISAC has added significant physical security threats and tactics to the NERC's biennial GridEx security exercises (discussed later in this report). In 2015,the E-ISAC also established a Physical Security Advisory Group, which includes industry physical security professionals, outside experts, and representatives from DOE and the Department of Homeland Security (DHS), to assist in the analysis of physical security threats and advise asset owners on physical threat mitigation. Through these efforts, the E-ISAC developed and ratified a design basis threat for the electric sector in December 2015.[46] The E-ISAC also has hosted two threat workshops, with plans for more.[47] Thus, while the E-ISAC has had no role in enforcing the CIP-014 standards, the security risk and mitigation information it develops and promulgates support the activities of bulk power asset owners complying with the standards.

FERC Oversight

As the agency with general statutory authority over grid reliability, and the agency which ordered and approved NERC's CIP-014 standard, the Federal Energy Regulatory Commission also oversees implementation of the standard. In carrying out this oversight, FERC relies primarily on annual compliance reporting by NERC.[48] However the commission also conducts some

[41] NERC, February 14, 2018.

[42] ISACs for critical infrastructure sectors were established under Presidential Decision Directive 63, May 22, 1998. NERC operates the E-ISAC in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC). The ESCC, established in 2004 by companies in the electric power industry, coordinates policy-related activities involving the reliability and resilience of the sector, including physical and cyber infrastructure.

[43] NERC, *Understanding Your E-ISAC*, June 2016, p. 3.

[44] NERC, "EOP-004-3—Event Reporting," 2015, http://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-3.pdf.

[45] NERC, June 2016, p. 3.

[46] NERC, *State of Reliability 2016*, May 2016, p. 7.

[47] NERC, *State of Reliability 2017*, June 2017, p. 62.

[48] FERC, *Order on Electric Reliability Organization Reliability Assurance Initiative and Requiring Compliance Filing*, Docket No. RR15-2-000, p. 11, February 19, 2015, http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/FERC_Order_Approving_Risk-Based_CMEP.pdf.

independent compliance activities, and it also conducts some compliance activities in cooperation with NERC. For example, during the initial rollout of the CIP-014 standard in 2016, FERC staff coordinated with NERC staff in support of on-site visits to the covered entities discussed above.[49]

In its order approving CIP-014-01, the commission stated that NERC staff would submit to both the NERC Board of Trustees and FERC a report following implementation of requirements R1, R2, and R3 about the scope, number, and characteristics of facilities identified as critical.[50] The order stated that

> Based on the results reported by NERC, we expect Commission staff to audit a representative number of applicable entities to ensure compliance with Reliability Standard CIP-014-1. Depending on the audit findings, the Commission will determine if there is a need for any further action by the Commission including, but not limited to, directing NERC to develop modifications to Reliability Standard CIP-014-1 to provide greater specificity to the methodology for determining critical facilities.[51]

As of November 2, 2017, FERC had completed two audits of critical assets identified by covered entities (R1) and was in the process of conducting a third. These audits have involved technical review of utility regulatory documents by FERC engineers. According to FERC staff, the initial audits identified one issue of concern related to the interpretation of specific language in the standard regarding asset criticality.[52] In addition to NERC's annual reports, FERC receives from NERC periodic Notices of Penalty (NOP) to regulated entities for reliability standards violations. As of November 30, 2017, FERC received NOPs for two violations (apparently at the same utility) of the CIP-014 standard.[53]

DOE Initiatives

Presidential Decision Directive 63 (PDD-63), issued during the Clinton Administration in 1998, established national policy for critical infrastructure protection from both physical and cyber threats.[54] PDD-63 established 15 critical infrastructure sectors. The Department of Energy was assigned responsibility for (1) the electric power, and (2) the oil and natural gas production and storage sectors. The George W. Bush Administration built on the work of PDD-63, superseding it in 2003 with Homeland Security Presidential Directive 7 (HSPD-7) on "Critical Infrastructure Identification, Prioritization, and Protection."[55] HSPD-7 again assigned to DOE (as a Sector-Specific Agency) responsibility for the energy sector—including electric power—as well as responsibility for being the federal coordinator for all critical infrastructure protection efforts.[56] The Obama Administration superseded HSPD-7 with Presidential Policy Directive 21 (PPD-21)

[49] NERC, May 2017, p. 16.

[50] FERC, *Physical Security Reliability Standard*, Docket No. RM14-15-000, Order No. 802, November 20, 2014, p. 23, http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Final%20Rule%20on%20CIP-014-1.pdf.

[51] FERC, Order No. 802, p. 24.

[52] FERC, Staff meeting with CRS analysts, Washington, DC, November 2, 2017.

[53] NERC, *Enforcement and Mitigation*, "Searchable NOP Spreadsheet," web page, accessed December 12, 2017, http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx.

[54] National Security Council and National Security Council Records Management Office, "PDD-63—Critical Infrastructure Protection," *Clinton Digital Library*, May 20, 1998.

[55] George W. Bush White House Archives, "Critical Infrastructure Identification, Prioritization, and Protection," Homeland Security Presidential Directive/HSPD-7, December 17, 2003.

[56] For details about the roles of Sector-Specific Agencies, see Department of Homeland Security, "Sector-Specific Agencies," web page, July 11, 2017, https://www.dhs.gov/sector-specific-agencies.

on "Critical Infrastructure Security and Resilience" in 2013.[57] PPD-21 retained the Sector-Specific Agencies (SSAs) from HSPD-7, with DOE continuing as the SSA for the energy sector. Thus, DOE has had a supportive role in helping utilities to protect bulk power critical assets over the last two decades.

Until recently, DOE's power grid security activities were led by its Office of Electricity Delivery and Energy Reliability (OE) within the Office of the Under Secretary for Science and Energy. A 2008 OE report stated that "OE's mission is to advance technology—in partnership with industry, government, academia, and the public—to meet America's need for a reliable, efficient, and resilient electric power grid."[58] Although the office was primarily focused on grid cybersecurity, it did conduct activities related to power grid physical security, including analysis of large power transformer security, a substation security awareness campaign, and efforts to support and coordinate research and development for physical security.[59] On February 14, 2018, DOE announced that the Secretary of Energy was establishing a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to be led by an Assistant Secretary with responsibilities to help protect energy infrastructure from "from cyber threats, physical attack and natural disaster."[60] How this reorganization will affect DOE's activities in bulk power physical security remains to be seen.

Observed Changes in Bulk Power Physical Security

Most grid security analysts consider the 2013 Metcalf substation attack to have been the "wake up call" which both changed electric sector attitudes toward grid physical security and motivated the promulgation of NERC's physical security regulations. Since that time, there have been a number of apparent changes within the electricity sector related to increasing bulk power physical security. It is not clear whether these changes have been driven more by changes in utility perceptions of grid threats or by NERC's mandatory security standards. Furthermore, there is currently no comprehensive accounting of changes in physical security throughout the sector. Nonetheless, anecdotal information in the public domain suggests that such changes may be significant and widespread. They are discussed in the following sections.

Corporate Structure Supporting Physical Security

One criticism that arose in the wake of the Metcalf attack was that physical security management at Pacific Gas and Electric Company (PG&E, the Metcalf substation's owner) and at other utilities was not a centrally organized or well-supported function in corporate management. This lack of support limited the influence of security managers in corporate planning and financial decisions.[61] However, it appears that many utilities have been reconfiguring and elevating

[57] Barack H. Obama White House Archives, "Critical Infrastructure Security and Resilience," Presidential Policy Directive-21, February 12, 2013.

[58] Department of Energy, Office of Electricity Delivery and Energy Reliability (Hereinafter OE), *National SCADA Test Bed Program, Multi-Year Plan FY2008-2013*, January 2008, p. 7.

[59] Department of Energy, Energy Sector-Specific Plan, 2015, pp. 16, 27. For discussion of OE's cybersecurity activities, see CRS Report R44939, *Cybersecurity for Energy Delivery Systems: DOE Programs*, by (name redacted), (name redacted), and (name redacted) .

[60] U.S. Department of Energy, "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response," press release, February 14, 2018.

[61] See, for example, Tony Kovaleski, Liz Wagner, and Mark Villarreal, "Internal Memo Reveals PG&E Years Away from Substation Security," *NBC Bay Area*, April 5, 2106, https://www.nbcbayarea.com/investigations/Internal-Memo-

physical security functions within their corporate structures. For example, owners of transmission assets such as PG&E, American Electric Power, and Xcel Energy have appointed Chief Security Officers at senior levels responsible for managing both physical and cyber security risks company-wide.[62]

> The senior security professional, typically at the vice president or director level, now has direct access to the [Chief Executive Officer] and company boards of trustees, often to supply situational awareness of physical and cybersecurity issues.… The electricity industry is quickly moving away from security as an "addition duty".… [M]ost utilities today have dedicated security departments committed to the protection of company assets and personnel.[63]

Utilities are also centralizing and bolstering their physical security capabilities at the operational level. Between 2014 and 2017, for example, Xcel Energy consolidated and grew its staffing for the "Chief Security Officer class of services" from 47 to 63 employees.[64] According to the company's regulatory filings

> the increase in average staffing levels ... was due to the need to correct a lack of resources to ensure adequate headcount to provide essential cyber and physical Enterprise Security services for Xcel Energy…. This increase in staffing demonstrates the emerging need that led to a stand-alone organization (i.e., the Chief Security Officer) to focus on Cyber Operations, Enterprise Resilience, Physical Security and Security Governance.[65]

Likewise, in response to the Metcalf attack, Dominion Energy established "a true cross-functional team with more than 100 people representing the entire Dominion organization," to develop and implement a more comprehensive substation security program.[66] Such efforts appear to extend to major publicly owned utilities as well. For example, according to the head of the Western Area Power Administration (WAPA), one of four federal power marketing administrations,

> WAPA's approach to physical security ... began in 2013 with the consolidation of our Office of Security and Emergency Management across our five regions and the implementation of a sophisticated risk-based program in analyzing the threats and vulnerabilities to our substations.[67]

The Tennessee Valley Authority (TVA), which operates federally owned hydroelectric and nuclear generation and associated transmission assets, recently closed a job posting for eight entry-level

---

Reveals-PGE-Years-Away-from-Substation-Security-303833811.html.

[62] PG&E Corp., "Bernard A. Cowens," web page, January 9, 2017, http://www.pgecorp.com/corp/about-us/officers/company/bernard-cowens.page; American Electric Power, "AEP Names Partlow Vice President & Chief Security Officer," press release, August 25, 2015; Xcel Energy, *Application of Southwestern Public Service Company for Authority to Change Rates*, Direct Testimony of Stephen J. Brown, filing with the Public Utility Commission of Texas, August 21, 2017, https://www.xcelenergy.com/staticfiles/xe-responsive/Company/Rates%20&%20Regulations/Rate%20Cases/Brown-RR-Direct.pdf.

[63] Brian Harrell, "The Modern Look of a Utility's Chief Security Officer," *CSO*, August 4, 2016, https://www.csoonline.com/article/3101474/leadership-management/the-modern-look-of-a-utilitys-chief-security-officer.html.

[64] Xcel Energy, Application of Southwestern Public Service Company for Authority to Change Rates, Update Testimony of Stephen J. Brown, September 27, 2017, p. 10, https://www.xcelenergy.com/staticfiles/xe-responsive/Company/Rates%20&%20Regulations/Rate%20Cases/13%20-%20BrownRRUpdate.pdf.

[65] Xcel Energy, August 21, 2017, p. 26.

[66] Bob McGuire et al., "Substation Security Is More Than Just a Fence," *T&D World*, September 28, 2015.

[67] Mark A. Gabriel, Administrator and Chief Executive Officer, Western Area Power Administration, "Physical and Cyber Threats," *T&D World*, May 8, 2017. Power Marketing Administrations (PMAs) operate electric transmission systems and sell power generated by federally owned hydroelectric dams across much of the United States.

Inspectors, each to be "trained as a physical security specialist" to provide "comprehensive security services, including assessments of facilities to identify credible threats, and implementation and testing of countermeasures to mitigate risks."[68]

Some transmission owners are also specifically increasing their in-house intelligence capabilities in physical security, including recent postings for positions such as "Security Intelligence Specialist" and "Director—Corp Security Info & Intelligence."[69] While the examples above are anecdotal, they would be consistent with what may be a trend among key grid owners to make physical security a better-organized and more influential corporate function. Not all utilities may be implementing such organizational changes, however.

Physical Security in Long-Term Transmission Planning

Since NERC promulgated the CIP-014 standards, some utilities have begun to put a greater emphasis on bulk power physical security as a design consideration in long-term transmission system planning. This approach aligns with the California Public Utilities Commission's recommendation in its 2018 report that, "there should be an emphasis on incorporating a menu of physical security strategies [into] any substation from the time of its inception."[70] For example, Public Service Enterprise Group's transmission planning criteria for its Long Island system in New York discusses the use of power system simulation tools for "various transmission system security and reliability studies."[71] Commonwealth Edison's transmission planning criteria includes a separate section on "security criteria" for system design which considers "severe low probability outage combinations" and seeks "to avoid cascading outages, instability, or widespread blackout."[72] Such criteria could apply to both natural and man-made outages, but they are consistent with, and readily applied to, design considerations for enhanced physical security. American Electric Power (AEP) also has incorporated asset criticality as a design criterion in its transmission planning.

> As a result of the revised NERC CIP standards, AEP now classifies all of its bulk electric system facilities based on the critical nature of the equipment to determine the level of security needed. This approach allows us to design security controls directly into new infrastructure from the start, building the costs into capital projects as needed. It also allows us to be more proactive with new and existing infrastructure while balancing risks with mitigation solutions.[73]

---

[68] Tennessee Valley Authority, "Inspector I–507038," job posting, *Linked-in JOBS*, web page, posted January 17, 2018, accessed February 1, 2018, https://www.linkedin.com/jobs/view/inspector-i-507038-at-tennessee-valley-authority-578188690.

[69] American Transmission Company, "Security Intelligence Specialist," job listing on *LinkedIn*, posted March 6, 2017, https://www.linkedin.com/jobs/view/security-intelligence-specialist-at-american-transmission-552328921; Avangrid, "Director—Corp Security Info & Intelligence," job listing on Glassdoor.com, posted January 3, 2018, https://www.glassdoor.com/job-listing/director-corp-security-info-intelligence-avangrid-JV_IC1148470_KO0,40_KE41,49.htm?jl=2630675613&utm_source=google_jobs&utm_medium=organic.

[70] CPUC, January 2018, p. 8.

[71] PSEG Long Island, "Transmission Planning Criteria," accessed January 10, 2018, p. 5, https://www.psegliny.com/files.cfm/TransmissionPlanningCriteria.pdf.

[72] Commonwealth Edison Co., "Transmission Planning Criteria," February 10, 2017, p. 10, https://www.pjm.com/-/media/planning/planning-criteria/commonwealth-edison-planning-criteria.ashx?la=en

[73] American Electric Power Corp., *2017 AEP Corporate Accountability Report*, "Cyber and Physical Security," web page, May 25, 2017, http://www.aepsustainability.com/about/security/cyber.aspx.

In its plans for a 2018 reliability-related upgrade at one its substations, Vermont Electric Power Company states that it "will also take the opportunity to make improvements to the physical security" of the substation.[74] According to NERC officials, based on security criteria, some utilities also have begun to consider new transmission interconnections not only to increase line capacity for bulk power flows, but also to reduce the criticality of particular transformer substations in congested areas by providing more transmission paths around them.[75]

New Security Products and Services

As utilities have devoted greater organizational and financial resources towards power grid physical security, industry vendors have been offering more physical security products and services to meet sector demand. As one utility services company has observed, "we can expect plenty of innovation as manufacturers see new markets due to the new standards for physical security of critical substations."[76] These offerings range from analytical services for security planning to physical products to harden physical assets. A comprehensive survey of such offerings is beyond the scope of this report, but the following examples illustrate the kinds of products now commercially available in the bulk power physical security market.

- **Security Program Planning and Implementation**. Engineering and security consulting firms have developed customizable programs specifically for power grid physical security review, planning, analysis, and implementation in compliance with the CIP-014 standards and utility-specific requirements.[77]
- **Anti-Intrusion Products**. Vendors have been marketing existing intrusion-related products specifically for use at bulk power critical facilities. These products include visual, acoustic, thermal radar, and electromagnetic systems for facility monitoring, intrusion detection, and response.[78]
- **Hardened Transformers and Components**. At least two major manufacturers have been marketing bulk power transformers with integrated ballistic shielding, or customizable plates to shield existing transformers.[79] Smaller manufacturers have also begun marketing hardened transformer components, such as composite bushings, for new and retrofit substation applications.[80]

[74] Vermont Electric Power Company, "East Avenue & Queen City Substation Improvement Project," web page, accessed February 1, 2018, https://www.velco.com/our-work/projects/project-east-avenue-queen-city-substation-improvement-project.

[75] NERC, December 7, 2017.

[76] Southwire Company, "Protecting the Grid," *T&D World*, sponsored content, May 15, 2017.

[77] See, for example, Burns & McDonnell, "Station Defender," web page, January 30, 2018, https://info.burnsmcd.com/station-defender/project-delivery; Corporate Risk Solutions, "Physical Security," web page, January 30, 2018, https://corprisk.net/physical-security/.

[78] See, for example, "How VTI Security Protected an Electrical Substation With a Radar-Thermal Imaging Solution," Security *Sales & Integration*, September 20, 2017, https://www.securitysales.com/in-depth/vti-security-radar-thermal-imaging-solution/; and i2c Technologies, Ltd., "Power Substation Protection," marketing brochure, May 2017, http://www.i2ctech.com/wp-content/uploads/2017/05/2509-i2cTech-CMYK.pdf.

[79] See, for example, Siemens AG, "First Bullet Resistant Retrofit Ordered for a Transformer," press release, January 28, 2018, https://www.siemens.com/global/en/home/products/energy/references/first-bullet-resistant-retrofit-ordered-for-a-transformer.html.

[80] Mike Sheppard and Saqib Saeed, "Bullet and Weather Concerns Driver of Retrofits in US Market," Power Technology Research LLC, October 26, 2017, https://powertechresearch.com/bullet-and-weather-concerns-driver-of-retrofits-in-us-market/.

- **Substation Perimeter Shielding**. A number of vendors have been marketing perimeter fencing and wall products specifically for visual and physical shielding of bulk power substations.[81] Most of these products are designed specifically to protect against rifle attacks such as the Metcalf attack.

Although new physical security products and services are being marketed in the utility sector, there is no comprehensive source of data about their sales to bulk power asset owners. Simply because vendors are marketing products does not mean that many utilities are buying them. For example, as of October 2017, Siemens Corp. had announced only one commercial order for its new transformer ballistic shielding retrofit product.[82] Thus, the overall impact of such offerings on the sector cannot be qualified reliably. Additional discussion of physical security spending is in the following section.

Capital Investment in Physical Security

Major changes in power grid operational expenses and capital investment are generally slow to occur. In privately owned utilities, significant changes in spending and plans for new capital projects may need to go through a number of rigorous screens, including power network modeling, a corporate capital allocation process, a regulatory approval process, and a procurement process. Publicly owned utilities may need approval from cooperative boards, or municipal or federal officials. This combination of requirements can take years to complete. Consequently, many significant operating expenditures or capital investments for physical security identified in security plans under CIP-014 may still be working their way through utility budgets and implementation. For example, in a 2016 rate filing, Southern California Edison stated that it planned to make physical security improvements at approximately 24 facilities in 2015-2017 and proposed to upgrade 8 substations per year from 2016 through 2020.[83] Likewise, in its 2016 annual report, Dominion Resources' timeline for power grid capital investment in "Physical Security" runs to 2021.[84]

Notwithstanding the potential length of time it may take for some security projects to be approved and implemented, there are indications in the public record that bulk power asset owners have already been spending more on new physical security measures. In its December 2016 report, the Edison Electric Institute stated that "primary factors driving transmission investment between 2015 and 2019" included "system hardening and resiliency to minimize adverse catastrophic events" and "improvements to comply with evolving transmission reliability and security compliance standards."[85] In its January 2018 white paper, the California Public Utilities Commission (CPUC) reports that investor-owned utilities under its jurisdiction "already ... have

[81] See, for example, Oldcastle, Inc., "How Precast Substation Walls Increase Power Grid Security," web page, https://www.buildingsolutions.com/industry-insights/how-precast-substation-walls-increase-power-grid-security; AFTEC LLC, "Substation Security Walls," web page, 2017, https://aftec.com/substation-security-walls/;

[82] Siemens AG, "First Bullet Resistant Retrofit Ordered for a Transformer," press release, October 17, 2017, https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/energy-management/medium-voltage-power-distribution/2017-10-17-tr-success-bullet-resistant-retrofit-v1-en.pdf.

[83] Southern California Edison Co., Application Of Southern California Edison Company (U 338E) For Authority To Increase Its Authorized Revenues For Electric Service In 2018, Among Other Things, And To Reflect That Increase In Rates, A.16-09-001, Before the Public Utilities Commission of the State of California, September 1, 2016, http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/9F664E3F0B77B7E488258195007C8F53/$FILE/SCE%20Opening%20Brief%20and%20COS.pdf.

[84] Dominion Resources, Inc., *Energy is Essential*, 2016 Summary Annual Report, 2017, p. 5.

[85] Edison Electric Institute, *Transmission Projects: At A Glance*, December 2016, p. vi.

sought approval for tens of millions of dollars in General Rate Case funding to ensure physical security."[86] The following examples illustrate the types of physical security projects and recent spending in publicly available sources.

- In 2017, the Bonneville Power Administration announced stand–alone plans to install security fencing at two high-voltage substations in compliance with NERC's security standards and to "protect critical assets from theft, vandalism, and terrorism."[87]
- In 2017, PPL Electric Utilities reportedly filed for regulatory approval for a $450,000 expenditure to reconfigure a 500 kV substation in compliance with NERC's CIP-014 physical security standard.[88]
- In 2017 regulatory filings, Vectren (Indiana) described plans to invest $2.9 million for physical security upgrades at critical substations, including enhanced fencing, access control, video surveillance, and perimeter motion detection.[89]
- According to the Western Area Power Administration, its expenses for physical security "nearly tripled" between 2013 and 2017.[90]

Utility Participation in Voluntary Security Programs

Although the CIP-014 mandatory physical security standards have only been in effect since 2014, bulk power asset owners have had earlier opportunities to participate in voluntary security initiatives administered by NERC and DHS. Utility participation in these voluntary programs is another indication of overall efforts in the sector to improve critical asset physical security.

NERC Grid Security Exercises

In 2011, NERC conducted GridEx, the first of an ongoing series of biennial electric sector-wide grid security exercises.[91] The 2011 exercise assessed the readiness of utilities to respond to a cyberattack, strengthened their crisis response, and provided input for internal security program improvements. Although the exercise was focused on a cyberattack, it did involve physical incursions into power grid substations as well as aspects of grid monitoring and recovery that would be relevant to an attack on critical transformers.[92] After the Metcalf attack in 2013, NERC conducted a second, more expansive grid security exercise, GridEx II. The exercise scenario

[86] California Public Utilities Commission (CPUC), *Security and Resilience for California Electric Distribution Infrastructure: Regulatory and Industry Response to SB 699*, January 2018, p. 5.

[87] Bonneville Power Administration, Categorical Exclusion Determination, "Proposed Action: Covington and Maple Valley Substations Perimeter Security Upgrades," April 27, 2017, https://www.bpa.gov/efw/Analysis/CategoricalExclusions/cx/20170427_Covington-and-Maple-Valley-Substations-Perimeter-Security-Upgrades.pdf.

[88] Corina Rivera Linares, "PPL Electric Utilities Seeks Approval of Two Projects in Pennsylvania," *Transmission Hub*, PennWell Publishing, May 22, 2017.

[89] Southern Indiana Gas and Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc. IURC Cause No. 44910, filing with the Indiana Utility Regulatory Commission, February 23, 2017, Attachment LKW-2, p. 31, https://iurc.portal.in.gov/_entity/sharepointdocumentlocation/b4477c28-00fa-e611-8104-1458d04e8ff8/bb9c6bba-fd52-45ad-8e64-a444aef13c39?file=44910_Vectren%20South_No%202_Direct%20Testimony%20and%20Attachments_Wilson_PUBLIC_022317.pdf

[90] Mark A. Gabriel, May 8, 2017.

[91] NERC's E-ISAC division organizes and administers its GridEx exercises.

[92] North American Electric Reliability Corporation (NERC), *2011 NERC Grid Security Exercise: After Action Report*, March 2012, p. i.

included a cyberattack on the grid coupled with a coordinated physical attack against a subset of transmission and generation assets—including critical transformer substations.[93] NERC conducted GridEx III in 2015, again including a baseline scenario with cyber and physical attacks, but also with an option for participants to customize the baseline scenario to meet local objectives.[94] NERC conducted its most recent exercises, GridEx IV, in November 2017.

According to NERC, one indication of progress in bulk power grid security is increasing participation by electricity sector entities in its GridEx exercises. The number of utilities participating in GridEx rose from 49 in 2011 to 166 in 2015.[95] NERC has not yet released participation details for GridEx IV, but the DOE reported that the latest exercise had more participants than in 2015.[96]

DHS Critical Infrastructure Surveys

The Department of Homeland Security's Protective Security Coordination Division conducts voluntary field assessments of critical infrastructure to identify vulnerabilities, interdependencies, capabilities, and cascading effects of potential terrorist attacks. As part of these efforts, DHS Protective Security Advisors offer voluntary, web-based security surveys of critical facility security using the agency's Infrastructure Survey Tool developed in 2008. The key goals of the surveys are to identify facilities' physical security and security management, identify security gaps, create facility protective and resilience measures indices that can be compared to similar facilities, and track progress toward improving security.[97] According to DHS officials, of more than 6,000 surveys completed since the program began, over 600 have been conducted on electric power facilities—although the timing of these surveys and the specific types of power facilities involved are not reported.[98]

Legislative Proposals in the 115th Congress

Given the relatively recent promulgation of NERC's new physical security standards, bulk power physical security has not been a major legislative focus in the 115th Congress. Nonetheless, several bills include provisions intended to enhance bulk power physical security—primarily by establishing new DOE grid security programs rather than by imposing new requirements on FERC or on bulk power asset owners directly. The relevant provisions of these bills, and a related resolution, are summarized below.

- The **Enhancing Grid Security Through Public-Private Partnerships Act** (H.R. 5240) would require DOE to establish a program to facilitate public-private partnerships for electric utility physical security and cybersecurity, among other provisions. Program activities would support voluntary implementation of

[93] NERC, *Grid Security Exercise (GridEx II): After-Action Report*, March 2014, p.15; Matthew L. Wald, "Attack Ravages Power Grid. (Just a Test.)," *New York Times*, November 14, 2013.

[94] NERC, *Grid Security Exercise: GridEx III Report*, March 2016, p. 7.

[95] NERC, March 2016, p. 1.

[96] U.S. Department of Energy, "GridEx IV: Government and Industry Exercise Together to Improve the Response to Grid Security Emergencies," November 21, 2017, https://energy.gov/articles/gridex-iv-government-and-industry-exercise-together-improve-response-grid-security.

[97] Department of Homeland Security, "Critical Infrastructure Vulnerability Assessments," web page, April 17, 2017, https://www.dhs.gov/critical-infrastructure-vulnerability-assessments.

[98] Daniel Genua, Department of Homeland Security, Presentation at George Mason University, Center for Energy Science and Policy, Grid Security Symposium, Arlington, VA, October 25, 2017, http://cesp.gmu.edu/wp-content/uploads/2017/10/UNCLASS_GMU-Panel-Presentation_25Oct2017_FINAL.pdf.

maturity models, self-assessment, and security auditing; sharing of best practices and data collection in the electric sector; and training and technical assistance to utilities (§2(a)).

- The **Energy Emergency Leadership Act** (H.R. 5174) would amend the Department of Energy Organization Act to include "energy emergency and energy security" to the functions assigned to Assistant Secretaries. These functions would include responsibilities with respect to emerging threats, supply, and emergency planning, among others. They would also include "provision of technical assistance, support, and response capabilities with respect to energy security threats, risks, and incidents" (§2).
- The **Energy and Natural Resources Act of 2017** (S. 1460) would require DOE to develop an advanced energy security program to secure energy networks, including electric transmission and delivery. Eligible activities would include developing "capabilities to identify vulnerabilities and critical components that pose major risks to grid security if destroyed or impaired," modeling national level impacts from human-made events, developing a physical security maturity model, conducting grid security exercises, conducting research on critical asset hardening, and other related measures (§2002(e)).
- The **Leading Infrastructure for Tomorrow's America Act** (H.R. 2479) would establish a grant program administered by DOE "to enhance energy security through measures for electricity delivery infrastructure hardening and enhanced resilience and reliability" (§31101(a)).
- The **Advancing Grid Storage Act of 2017 (**S. 1851**)** would establish a competitive grant program for pilot energy storage systems administered by DOE with one objective being to "improve the security of critical infrastructure and emergency response systems" in the electric grid (§5(a)(4)(A)).
- The **Grid Cybersecurity Research and Development Act** (H.R. 4120) would require DOE, together with bulk power asset owners, and in collaboration with the National Laboratories, to "utilize a range of methods, including voluntary vulnerability testing and red team-blue team exercises, to identify vulnerabilities in physical and cyber systems" (§6(a)).
- The **Flexible Grid Infrastructure Act of 2017 (**S. 1875**)** would require DOE to: develop model standards for the electric distribution grid, in part to improve security with respect to physical threats (§5(d)(1)), evaluate whether new performance standards and testing procedures are needed to ensure electrical equipment resilience in the face physical threats (§5(d)(2)), and submit to Congress methods and guidelines for calculating the costs and benefits of investments in resilience and security solutions for the electric grid (§5(e)(1)).
- **House Resolution 334** states that it should be the policy of the United States to, among other things, "bolster the reliability, affordability, diversity, efficiency, security, and resiliency of domestic energy supplies, through advanced grid technologies," and to promote advanced grid tools "to increase data security, physical security, and cybersecurity awareness and protection."

Policy Issues for Congress

Although NERC's CIP-014 standards have been promulgated, and bulk power asset owners have begun enhancing physical security, Congress continues to be concerned about the current state of

electric grid physical security. Among many issues of potential interest, Congress may focus on several with overarching policy significance: security implementation oversight, cost recovery, hardening vs. resilience, and the quality of threat information.

Oversight of Physical Security Implementation

Although FERC's statutory authority for grid reliability and NERC's reliability standards both include provisions for oversight and enforcement, congressional oversight of physical security implementation may be a challenge for several reasons. First and foremost, information about physical security measures is inherently sensitive and there are both statutory and regulatory restrictions on its disclosure.[99] Therefore, the level of security-related information that utilities are willing or able to provide outside the CIP-014 third-party review process or NERC compliance audits is more limited than reports about, say, general reliability or safety.

NERC is not compiling a centralized database of critical assets or security measures implemented by the utilities subject to its physical security standard. Moreover, while NERC may provide security information to FERC, the security-related information NERC can provide in public reports is limited and typically redacted. Therefore, although information about CIP-014 implementation exists among the utilities and independent third parties (operating within the standard), and is provided at some level of specificity to NERC, that information may not be as useful or visible as it could be to Congress or other outside entities.

Another oversight challenge arises because NERC's CIP-014 standards are not prescriptive; bulk power asset owners have considerable discretion in the nature and timing of the physical security measures they may include in their physical security plans. NERC viewed such flexibility as necessary for its standard due to the unique characteristics of each utility's bulk power system and the risks it faces. However, this flexibility also may make it more difficult to develop useful metrics for CIP-014 implementation and comparing implementation among asset owners. NERC's standards for power grid physical security may ensure considerable consistency in the *process* utilities must undertake to identify critical substations and develop plans to secure them. However, they may not ensure consistency among the various security plans nor in the specific measures the individual asset owners will choose to implement to reduce the risk of intentional attacks. For example, ballistic shielding at critical substations may be an appropriate and sufficient protective measure for some utility assets, say, in open and rural areas, but not necessarily in more urban areas.

Even when detailed company-specific information about physical security measures is available, it might be difficult to develop reliable metrics to evaluate it. Metrics are an important tool NERC uses to evaluate utility performance in the context of power grid reliability.[100] However, officials at EEI have stated that measuring the adequacy of grid security for a diverse set of asset owners under changing risk circumstances poses significant problems. "Security metrics (for both cyber and physical security) have consistently been a challenge due evolving threats and vulnerabilities. If you build an eight-foot fence, the attacker just needs to bring a nine-foot ladder."[101] NERC is actively engaged in efforts to develop bulk power system security metrics in which it has likewise

[99] FERC regulations for the submission, designation, handling, sharing, and dissemination Critical Energy/Electric Infrastructure Information (CEII) are at 18 C.F.R. §388.113.

[100] See NERC, "Reliability Indicators," web page, http://www.nerc.com/pa/RAPA/Pages/ReliabilityIndicators.aspx.

[101] Chris Hickling, Edison Electric Institute, "RE: CIP-014 Implementation Update," email to CRS, October 30, 2017.

encountered "challenges associated with developing relevant and useful security metrics that rely on data willingly and ably provided by individual entities."[102]

Congress may judge the effectiveness of the CIP-014 physical security standards as best it can based on reports and testimony from NERC and FERC as well as information from the assets owners themselves. However, due to the issues above, if Congress decides the information as currently structured is insufficient to draw reliable conclusions about the status of bulk power physical security as a whole, it may revisit how the responsible agencies collect, measure, and report it. Congress may also consider additional avenues for reviewing this information, for example, through classified briefings or specifically requested studies or reports. Also, as FERC continues to implement its policy of regulating physical security of the power grid, Congress may examine whether company-specific security initiatives appropriately reflect the risk profiles of their particular assets, and whether additional security measures across the grid overall uniformly reflect terrorism risk from a national perspective.

Financial Requirements and Cost Recovery

Two of the barriers to physical security investment among utilities prior to the Metcalf attack were competition for limited capital investment resources and justifying security spending to corporate boards and utility rate regulators. NERC regulatory requirements for physical security make it easier for security managers to justify related operating and capital expenditures to corporate leadership, and to seek cost recovery for such expenditures through regulated rates. However, even where regulators have been supportive of cost recovery for physical security investments in general, they have faced challenges gauging the prudence of specific security investments because they are hard to evaluate on a traditional benefit-cost basis. As a 2006 report from the Electric Power Research Institute states,

> Security measures, in themselves, are cost items, with no direct monetary return. The benefits are in the avoided costs of potential attacks whose probability is generally not known. This makes cost-justification very difficult.[103]

Note that cost-justification requires not only the approval of utility management, but also of FERC and potentially state public utility commissions which regulate the rates grid owners may charge for electric transmission and distribution service. Regulators are responsible for ensuring that electricity rates are just and reasonable. They must be convinced that any new grid security capital costs and expenses are necessary and prudent before they will allow them to be passed through to ratepayers. However, corporate financial processes differ from utility to utility, and utility rate regulation differs from jurisdiction to jurisdiction, so investment and cost recovery for physical security is not uniform across the electricity sector and remains a work in progress. As implementation of new physical security plans under CIP-014 continues, Congress may examine whether the overall level of investment appropriately reflects the level of security risk facing the bulk power system, and whether any cost-recovery barriers are preventing assets owners from making investments necessary to secure the grid.

[102] NERC, *State of Reliability 2017*, June 2017 p. vii. For an expansive discussion of NERC's efforts to develop security metrics, see Appendix G in this NERC report.

[103] Electric Power Research Institute (EPRI), *Technologies for Remote Monitoring of Substation Assets: Physical Security*, March 2006, p. viii.

Hardening vs. Resilience

There are two fundamental approaches to reducing the risk of a successful physical attack on the electric grid. The first approach, which is the principal approach of NERC's CIP-014 standards, is to prevent attacks by monitoring critical facilities to identify would-be attackers before they attempt an attack, preventing attacker access to critical assets, and otherwise hardening facilities to make them more physically secure to protect against attack and equipment failure. The second approach is to make the broader power system more "resilient" to a successful attack on particular assets through an enhanced ability to manage loads, reroute power flows, and access other sources of generation to reduce the potential of blackouts even if critical assets are disabled.[104] Initiatives such as the spare transformer program administered by the Edison Electric Institute (EEI, the electric utility trade association), and a proposed federal Strategic Transformer Reserve, which can accelerate replacement of critical transformers if they are damaged, may contribute to the power grid's ability to sustain a terrorist attack without widespread grid failure.[105] Thus, while hardening is aimed more at reducing the likelihood of a successful attack, resilience aims at reducing potential consequence; doing either reduces overall security risk.

Measures to harden critical facilities and measures to increase system resilience are not exclusive of one another. In fact, they can be complementary in reducing overall security risk. However, they may involve different approaches to power grid operation and design, and they may involve different, competing types of investment (e.g., transformer shielding vs. transmission network sensors). Balancing the two approaches to most efficiently achieve a desired level of physical security is a challenge for utilities with limited capital budgets. The CPUC stated that "determining appropriate security measures or approaches to ensuring resiliency" was one of three "major issues" in its power grid physical security proceedings.[106] As Congress continues its oversight of bulk power physical security regulation, it may consider whether the electric power sector as a whole is striking an appropriate balance between these two approaches.

Threat Information

The utility industry's physical security risk assessments rely upon threat information from the federal government, among other sources.[107] The quality of this threat information is a key determinant of what bulk power asset owners need to be protecting against and what security measures to take. Incomplete or ambiguous threat information may lead to inconsistency in physical security among grid owners, inefficient spending of limited security resources at facilities (e.g., that may not really be under threat), or deployment of security measures against the wrong threat.

---

[104] For a discussion about power grid resiliency and associated federal efforts, see *Government Accountability Office, Electricity: Federal Efforts to Enhance Grid Resilience*, GAO-17-153, January 2017.

[105] For details about electric sector spare transformer programs, see Department of Energy, *Strategic Transformer Reserve*, report to Congress, March 2017.

[106] CPUC, January 2018, p. 5.

[107] Much of this information is communicated primarily through the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the sector's communications channel for security-related information, situational awareness, incident management, and coordination. The ES-ISAC was established under Presidential Decision Directive 63, May 22, 1998. The ES-ISAC is operated by NERC in collaboration with the DOE and Electricity Subsector Coordinating Council. Members may anonymously share information by means of a secure Internet portal. Registered users receive information on security threats and alerts, remediation, task forces, events, and other security-specific resources.

As discussed earlier in this report, the E-ISAC plays a valuable role in identifying and analyzing physical security risk, and disseminating information about those risks to bulk power asset owners. Independent third-party verification of risk assessments under the CIP-014 standards, together with NERC compliance audits, are two additional means of helping to ensure greater consistency of threat information among utilities. Nonetheless, a changing threat environment continues to pose challenges for physical security planning and investment. As NERC stated in a recent compliance report, "the security threat landscape is constantly changing and requires adaptation and information sharing on how best to address these issues in an effective and efficient manner."[108]

Concerns about the quality and specificity of federal threat information have long been an issue across all critical infrastructure sectors.[109] Threat information continues to be an uncertainty in the case of power grid physical security. For example, although there is wide consensus that the Metcalf attack was extremely alarming, some industry analysts have opined that FERC's physical security order nonetheless may have been an "overreaction" to Metcalf.[110] By contrast, former DHS Secretary Michael Chertoff has predicted that "the sophistication and resulting damage of the Metcalf attack will ... be exceeded" in a future attack.[111] Still others have expressed concern that FERC's physical security concerns may be too heavily focused on another Metcalf-type scenario—the last threat—rather than a wider range of potential future threats.

As discussed earlier, there is widespread belief that bulk power critical assets are vulnerable to physical attack, that such an attack potentially could have catastrophic consequences, and that the risks of such attacks are growing. But the exact nature of such potential attacks and the capability of perpetrators to successfully execute them are uncertain. Consequently, despite the technical arguments, with limited information about potential targets and attacker capabilities, the true vulnerability of the grid remains an open—and evolving—question. As Congress seeks to establish the best policies to address bulk power physical security, it may examine how federal and electric sector threat information is developed and used by critical asset owners, and how limitations and uncertainty of this information may affect physical security of the electric grid.

Conclusion

The 2013 attack on the Metcalf transformer substation marked a turning point for the U.S. electric power sector. The attack prompted utilities across the country to reevaluate and restructure their physical security programs. It also set in motion proceedings in Congress and at FERC which resulted in the promulgation of NERC's CIP-014 mandatory physical security standards in 2015. Based on discussions with FERC and NERC staff about utility compliance, as well as a review of public information about the activities of bulk power asset owners (and the vendors supplying them), there appear to be physical security improvements underway among owners of bulk power critical assets. The public record is too anecdotal to assert conclusively that these changes are occurring uniformly and at every relevant utility, but NERC's summary compliance reports so far

[108] NERC, *Compliance Monitoring and Enforcement Program Quarterly Report, Q3 2017*, November 8, 2017, p. 8.

[109] See, for example, Philip Shenon, "Threats and Responses: Domestic Security," *New York Times*, June 5, 2003, p. A15.

[110] Deborah Carpentier, "NERC Gains in Vegetation Management, Cyber and Physical Security, and Reliability Assurance," *Natural Gas & Electricity* (Wiley Periodicals), May 2014, p. 31, http://www.crowell.com/files/NERC-Gains-in-Vegetation-Management-Cyber-and-Physical-Security-and-Reliability-Assurance.pdf.

[111] Michael Chertoff, "Building a Resilient Power Grid," *Electric Perspectives*, May/June 2014, p. 35.

have been positive, especially for such a new standard. As NERC concluded in its *State of Reliability 2017* report

> What NERC can measure is that no major cyber- and few physical-related load losses have happened to date; that extremely low numbers of incidents have occurred on the operating side, and that attention to security performance has been excellent on the corporate side.[112]

Although the electric power sector seems to be moving in the direction of more extensive physical security, many measures have yet to be implemented and the process of corporate realignment around physical security is still underway. As the CPUC has stated,

> It appears that the North American electric industry is in intermediate stages of fully harnessing the potential of security technologies and staff expertise, and integrating security and risk assessment values into the utility culture such that utility physical security ultimately is prioritized on par with safety and reliability.[113]

Therefore, although it is probably accurate to conclude that, based on the objectives of the CIP-014 standards, the U.S. electric grid is more physically secure than it was five years ago, it has not necessarily reached the level of physical security needed based on the sector's own assessments of risk. Bulk power physical security remains a work in progress. As CIP-014 implementation and other physical security initiatives proceed, Congress may seek to maintain its focus on the power sector's overall progress, not only on short term compliance with NERC's security standards, but also on structural changes supporting physical security as a priority far into the future.

Author Contact Information

(name redacted)
Specialist in Energy and Infrastructure Policy
[redacted]@crs.loc.gov , 7-....

[112] NERC, June 2017, p. 59.

[113] CPUC, January 2018, p. 57.